

NO. 21
December 2011 • Price Free • www.networkset.net
NetWork Set
First Arabic Magazine For Networks
10
أخطاء
يجب تجنبها
عند تشغيل
الكابلات
في شبكتك
تحكم بسطح المكتب
بشكل كامل من خلال
متصفح الانترنت
تلفزيون الانترنت
كيف تحمي شبكتك
Real Time
Transport Protocol
Radio roles in cisco
bridges
سيرفر المايكروتك
Gns3 Error 209
شهادة شكر وتقدير
للمهندس أحمد غزال

تحرروا من سيطرة سيسكو

طرحت منذ فترة وجيزة مقال يتحدث عن سياسة سيسكو الجديدة المتعلقة بعالم الرخص ومبدأ التحكم في الخواص والأمكانيات التى تحتاجها في عملك على الشبكة وكان هدف المقال العام هو الأشارة إلى فكرة التحرر من سيسكو ومن عالمها ومقالي اليوم سوف أخصصه للحديث عن هذه النقطة وما مدى أهميتها , بدأ مشوار تحرري من سيسكو مع بداية تعرفي على عالم جونيبر الذي وضح لي أن الشبكات لاتعني سيسكو فقط , لكن بقيت سيسكو معلقة في رأسي حتى مررت باحد التجارب العملية , التجربة كانت فترة تدريبية قضيتها في أحد الشركات الكبيرة التى تقدم حلول تقنية في مجال الشبكات وكان لدي أختبار صغير أمام مهندس هندي وأختباره كان عبارة عن سؤال واحد فقد , لدينا شركة تحتاج حل لربط فروع ببعضها البعض وهي تطلب منك تقديم حلول عملية في عملية الربط بحيث يكون الحل هو المثالي لهذه الشركة من خلال أقتراح الاجهزة التى سوف تعمل على الربط بين الفروع ؟ وهنا بدات أفكر بالحلول الممكنة ووجدت نفسي لا أعلم إلا سيسكو , فسألته هل هناك منتجات معينة يجب الاختيار منها ؟ فقال لي أختر ماتشاء لكن لانريد أجهزة سيسكو فالشركة لاتملك ميزانية كبيرة !!!. وهنا تبسمرت وبدأت افكر بشركات آخرى ومر على رأسي الكثير من الشركات لكن لا اعلم له ولامنتج واحد أستطيع عرضه بأستثناء جونيبر التى أعلم بعض منتجاتها لكن لن تناسب طلبهم كون جونيبر تملك ثغرة كبيرة في منتجاتها وهي التنوع بين متطلبات العمل وخصوصا أنها تركز على الاجهزة الثقيلة الحجم والأداء , وهنا بدأت أعي مشكلتي الحقيقية مع سيسكو , فالمشكلة أكبر من ذكر المنتجات وأرقامها بل بالأطلاع عليها فقط فأنا لن أحفظ أرقام وأنواع لكل الشركات لكن يتوجب علي معرفة هل لهذه الشركات حلول مع الـ Wan optimization أم لا ؟ وهو ما أخبرني به المهندس الهندي .

التجربة الثانية كنت انا من سن القاعدة فيها وأعرضها عليك علها تفيدك يوما ما فهي الشيئ الذهبي الذي أتشبث به أثناء إجراء المقابلات الشخصية وهو سؤالي حول معرفتي بالتعامل مع شركة أو منتج مثل 3Com أو Extreme والخ . . . وكنت أجيب دائما بأني مهندس شبكات أملك المبادئ العلمية والأسس التى يقوم عليها عالم الشبكات وفكرة تعلم كل الأنظمة الموجودة شيئ صعب حتى سيسكو نفسها لا أحفظ أي أوامر ولكن أعلم ماهي الخطوات التى يتوجب علي تنفيذها لتفعيل شيئ ما وهو نفس الأمر الذي ينطبق على اي منتج آخر .

حالي السابق هو حال نسبة كبيرة جدا من المهندسين والمتخصصين في مجال الشبكات الآن فنحن نولد في عالم سيسكو ولانرى إلا سيسكو بينما العالم الخارجي بدأ يتحرر منها تدريجيا , فلو تحدثنا في بعض التفاصيل العملية التى تجري الآن نجد أن سيسكو فقدت عالم السكيورتي تماما فهي لاتملك إلا حل واحد إسمه ASA وسعره خيالي مقارنة بمنتجات آخرى وخصوصا لو أخبرتك أن لكل خاصية أو ميزة تحتاج تركيبها هناك رخصة وسعر وهي موجودة قبل وجود النظام الجديد من سيسكو (15) , أما لو تحدثنا في عالم الفويب نجد شركة أفايا فرضت نفسها بقوة في عالم المبيعات , بينما نجد شركة Extreme تدخل مجال السويتشات وتضع لنا حلول مميزة وبأسعار مناسبة وباداء عالي . . . العالم بدأ يدرك أن المنافسة مع سيسكو مستحيلة فهي تشكل حوالي 70 ٪ من شبكات العالم لذلك أوجدوا الحل وهو التخصص في مجالات معينة فسيسكو من أقدم الشركات ولديها حلول مختلفة تناسب كل الاحتياجات لكن تشبثها بوجهة نظرها القائمة على مبدأ « لايمكن إيجاد منافس » وفرض سياسات جديدة مادية جدا بدأ يثمر إيجابيا مع بعض الشركات الآخرى , وقبل كتابتي لهذا المقال قررت البحث عن آخر الأحصائيات في عالم المبيعات ووجدت الكثير منها يشير إلى تراجع مبيعات سيسكو إلا أنني أعتبرت أغلبها مسيس لكن أستطيع أن أقر بوجود شركتان تنافسان سيسكو الآن وهما HP , و Huawei .

وأنت أخي العزيز توقف عن التفكير في سيسكو ولو ذهبت إلى أي مقابلة عمل لاتنطق باسمها وأجعل نفسك متوازنا مع جميع الحلول , لأن لكل طلب هناك أمور يجب توضيحها وهي مايجب عليك أن تركز وتفكر فيه وهي النقاط التقنية , فهي التى سوف تفتح لك المجال لتتعلم وتتأقلم مع كل المنتجات وطبعا سوف تتحرر من سيسكو ودمتم بود .

أيمن النعيمي - سوريا





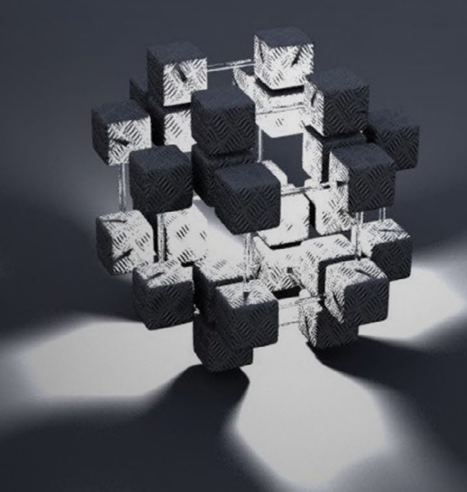
مجلة NetworkSet مجلة الكترونية شهرية متخصصة تصدر عن موقع www.networkset.net

www.networkset.net



NetWork Set

First Arabic Magazine For Networks



NetWork Set

معنى جديد لعالم الشبكات في سماء اللغة العربية













تلفزيون الإنترنت





هو تقنية بث القنوات التلفزيونية والبرامج والأفلام عبر شبكة الإنترنت, وتتنوع الأجهزة التي تتلقاها مابين أجهزة كمبيوتر متصلة بالإنترنت وكذلك أجهزة تلفزيون لديها اتصال شبكي بالإنترنت ويتم ذلك من خلال برمجيات داخلها تتلقى بيانات البث التلفزيوني عبر شبكة الإنترنت, وتنتشر هذه التقنية عبر شبكة الإنترنت التقليدية وتتطور بشكل يمكنها الوصول إلى كافة الأجهزة المحمولة أو الكفيّة, ومن الطبيعي أنّ المواقع التي تبث القنوات الفضائية هي ليست تطبيقاً لهذه التقنية, بل إنّ هذه التقنية تكون قد خصصت للبث عبر الانترنت من قِبَل القناة, وتختلف تقنياً كلياً كذلك .

وسنستعرض أهم التقنيات والأجهزة المتوافقة مع هذه التقنيات وهو جهاز تلفزيون سامسونج بتقنية Smart Hub

أنواع المعلومات التي يتم بثها باستخدام هذه التقنية

1. محطات تلفزيونية عالية الدقة أو تقليدية, وفي حال كون القناة تبث بتقنية HD فإنّ سرعة الاتصال المطلوبة يجب ألّا تقل عن 8 ميغا بت في الثانية لتتمكن من توصيل البيانات بالشكل المناسب
2. شبكات إخبارية تقدم الأخبار والتقارير بشكل مستمر.
3. الألعاب التشاركية والمتطورة.
4. برمجيات الإنترنت, كبرمجيات المحادثة وبرمجيات مشاركة الملفات والوسائط المتعددة.
5. تقنية النصوص (التلتيكست).

التقنيات المشابهة وأوجه الاختلاف

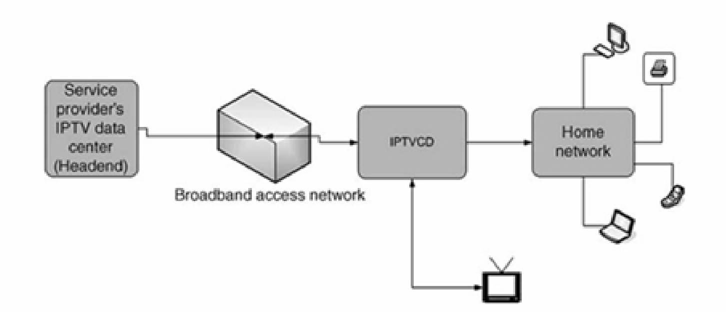
برزت مع تطور هذه التقنية تقنيات مشابهة تقوم بتوصيل البث التلفزيوني للمستخدمين ولكن مع فروقات مهمة عن تقنية تلفزيون الإنترنت, ومن أهم هذه التقنيات هي تقنية IPTV والتي تعمل على بث القنوات العالية الوضوح, وهي بذلك تشابه الفكرة العامة لتلفزيون الإنترنت ولكنها بالرغم من الانتشار الواسع والسريع لها فإنّها لا تزال محدودة الانتشار بالمقارنة مع التلفزيون التقليدي,

وإذا أردنا سرد أهم الفروقات بين التقنيتين فيمكننا الحديث عن :

1. بيئة عمل مختلفة, حيث تعمل تقنية IPTV على شبكة مخصصة تزوّد به الشركة مستخدميها.
2. IPTV هي تقنية مدفوعة وبرغم المنافسة إلّا أنّ أسعارها لا يستهان بها, أما تقنية تلفزيون الإنترنت فإنّها متاحة للجميع بما أنّ لديك أجهزة الاستقبال المناسبة.
3. مادامت شبكة IPTV هي شبكة مستقلة, فهي شبكة مضمونة الجودة عكس تلفزيون الإنترنت الذي قد تختلف جودته باختلاف ظروف الشبكة وجودتها .

ولقد انتشرت الشركات المزودة لمثل هذه التقنيات بكثرة في أوروبا وأمريكا والخليج العربي, وتوفر إمكانية الاتصال الهاتفي والإنترنت بسرعات عالية بالإضافة للوصول لقنوات مشفرة تبث بتقنية الصورة العالية الدقة Full HD وتعرف بتقنية الاشتراك بالكابل Via CablesInternet TV

ويمكننا من خلال الصورة التالية التعرف ببساطة إلى أساسيات هذه التقنية



وكذلك فإنّه قد يتبادر للذهن أنّ ما تبثه بعض المواقع من قنوات تلفزيونية بتقنية البث المباشر تعتبر تطبيقاً للإنترنت تي في, وهذا فهم خاطئ للتقنية حيث أنّ ما نراه في بعض المواقع من بث للقنوات ما هو إلّا عملية وصل لروابط مشاركة للبث التلفزيوني التقليدي عبر الإنترنت, ويمكن للمستخدم الوصول إلى العديد من القنوات الفضائية ولكن هنا تكون الجودة ضعيفة وكذلك الدقة, وتتمتع هذه التقنية بالإمكانيات الخاصة باختيار البرنامج أو التسجيل التي تتمتع بها أجهزة Internet TV

آلية العمل

يتطلب استخدام التقنية الجديدة اتصالاً سريعاً بالإنترنت عبر خط المشترك الرقمي DSL مثلاً، حيث يتم استخدام جهاز صغير يوصل إلى الإنترنت, ويكون هذا الجهاز مسؤولاً عن إعادة تجميع حزم البيانات ومن ثم فك تشفير هذه البيانات للحصول على محتويات الفيديو الأصلية، وقد يكون من الممكن تضمين هذا الجهاز ضمن الكمبيوتر ليقوم بهذه الوظيفة، ومع الحاجة المتزايدة لوجود سرعات كبيرة لنقل البيانات مع تطور تقنية البث التلفزيوني ذات الدقة العالية تم اللجوء إلى تقنيات ضغط البيانات أثناء البث مما يوفر نفس الجودة مع كمية أصغر من البيانات المتدفقة عبر الشبكة العنكبوتية, وأهم صيغ الفيديو التي تم الاعتماد عليها مع هذه التقنية هي صيغة MPEG مما يدعم وصول حجم أكبر من البيانات المضغوطة, وأداء أسرع وأفضل.

مزايا تميّز هذه التقنية عن التلفزيون التقليدي

تقدم هذه التقنية إمكانية متابعة البرامج المسجلة, وإمكانية إعادة عرض أي مقطع بشكل متكرر, كما تعتبر حلاً أمثل للحصول على قنوات قد لا يصل بثها الاعتيادي إلى بعض المناطق, كما يتضمن إمكانيات التصفح والتمتع بألعاب شبكيّة وعالية الدقة, وكذلك الكثير من التطبيقات الأخرى غير تلك التي يوفرها التلفزيون العادي مثل تطبيقات Youtube – Skype– Facebook .

أجهزة متوافقة مع هذه التقنية

كما أسلفنا بإمكاننا وصل أجهزة حاسوبية مزوّدة بجهاز للاتصال بهذه الخدمة, وكذلك فقد أصبحت معظم أجهزة التلفزيون الحديثة تدعم الاتصال الشبكي وما يسمى بتقنية Internet TV ومن هذه الأجهزة تلفزيون سامسونج D8090 .



سامسونج D8090 تلفزيون الانترنت

كأحد أهم الرواد في هذه التقنية فإنّ الصانع الكوري سامسونج أبدع في تطوير سلسلة من الأجهزة التلفزيونية المتطورة التي ترضي زبائنه, وسنستعرض أهم المميزات التي زوّد بها هذه الأجهزة لتكون تلفزيونات إنترنت وتلفزيونات تقليدية بنفس الوقت.

بدايةً تسمى هذه التقنية في أجهزة السامسونج تقنية SMART HUB, وهذه التقنية تسمح له بالولوج إلى الكثير من الأقنية المجانية عبر الدخول لقائمة Smart ومن ثم سوف تظهر لديك قائمة بأهم التطبيقات البرمجية التي تتيح لك مشاهدة قنوات تبث عبر الإنترنت, وتنقسم التطبيقات الموجودة ضمن هذه القائمة إلى تطبيقات لقنوات تلفزيونية ومن أشهرها BBC NEWS , وبإمكانك بمجرد توصيل التلفزيون سلكياً أو لاسلكياً الولوج المجاني للقناة التي تعرض نفس برامج قناتها العالمية, ولكن مع إمكانية عرض البرنامج عدة مرات واختيار البرنامج المراد مشاهدته, بالإضافة إلى أهم القنوات الشهيرة بعرض الأفلام والموسيقى مثل Acertrax movies المتخصصة في الأفلام.

تطبيقات للمواقع الشهيرة وهنا بإمكاننا الدخول لحسابنا على الفيس بوك , وكذلك انضم برنامج المحادثة الشهير إلى التطبيقات المتوفرة عبر هذا الجهاز, وبالإمكان محادثة الأصدقاء عبر كاميرا يمكن شراؤها من متاجر سامسونج خاصة للعمل مع البرنامج الشهير, وكذلك برنامج خرائط غوغل لمشاهدة الطرقات ومعرفة الاتجاهات تماماً كما نجده في الموبايل, بالإضافة لتطبيق اليويتوب, حيث يمكننا من خلاله مشاهدة أهم الفيديوهات بنفس طريقة استخدامنا لليوتيوب على الكومبيوتر ولكن مع الشاشة العملاقة فالرؤيا مختلفة.

تطبيقات تدعم إمكانية اختيار قنوات للمشاهدة ومصنفة وفقاً لأنواعها, من قنوات موسيقية أو أطفال أو إخبارية مثل Tv Digital أو viaway , والذي يعتبر من أشهر التطبيقات لعرض أهم القنوات التلفزيونية عبر تقنية البث عبر الإنترنت.

تطبيقات خاصة بالألعاب, وبرمجيات خاصة بتحويل العملات ومعرفة الطقس, بالإضافة إلى قنوات التسوق مثل Ebay وغيرها .

كما تجدر الإشارة إلى أنّ العديد من التطبيقات من الممكن إضافتها فورياً من خلال الدخول إلى تطبيقات سامسونج والبحث عن التطبيق حسب تصنيفه, وتقوم سامسونج دائماً بطرح التطبيقات الجديدة مجاناً للزبائن.

إمكانيات أخرى لتلفزيون الإنترنت

بالإضافة إلى كونه يقوم بعرض القنوات التلفزيونية, فإنّ وصوله للشبكة المحلية والعالمية يعطيه ميزة إمكانية الوصول للأجهزة المشتركة معه بالشبكة, وكذلك إمكانية اللعب عبر الإنترنت مع أشخاص موجودين على الإنترنت في أماكن أخرى, ولقد لفت نظري تطبيق موجود في هواتف السامسونج وهو All Share , حيث يوجد هذا التطبيق في كل من التلفزيون السابق وأجهزة النقال الحديث من سامسونج, وبالإمكان الدخول لهذا التطبيق مثلاً من خلال الهاتف بعد تشغيل الشبكة اللّاسلكية للولوج للشبكة المحلية, وهنا يمكن تشغيل أي صورة أو فيديو أو تطبيق وعرضه لاسلكياً عبر شاشة التلفزيون العملاقة.

هذا كله يقع ضمن تقنية Smart Tv, وهي تقنية تسمح للتلفاز بالوصول للإنترنت كأي حاسب, وتشغيل تطبيقات مختلفة, وحتى تصفح مواقع الإنترنت في الإصدارات المتقدمة من هذه الأجهزة.



يمكننا ببساطة التنبؤ بأنّ البث عبر الإنترنت قريباً سيسيطر على تقنية البث التلفزيوني, وخصوصاً إذا ما لاحظنا حجم التطور في سرعات الوصول للإنترنت من جهة, بالإضافة لتطور تقنيات البث التي أصبحت ترسل معلومات عالية الدقة بحجم أصغر, مما يضمن الوصول بالشكل الأمثل لشريحة كبيرة من المشاهدين دون الحاجة لسرعات اتصال خيالية كما في السابق.



DMZ ونظرة عن قرب

تخيل أنّك network admin و أنّ الشبكة كلها تحت سيطرتك, ومطلوب منك عمل security على الـ network , فمن أهم الخطوات التي ستبدأ التفكير بها هي شكل الـ network , بحيث أنّك ستقسمها و تقول في نفسك أنا سأقسمها لـareas , وأرى كل area بنسبة كم ٪ تمثل لي من vulnerability , بحيث تُمكّن أي attacker من تنفيذ successful attack , وتبدأ بتحصين الأماكن التي تحتاج security أعلى, سواءً بـ devices أو configurations وهكذا... , وبذلك تكون قد أنجزتconcept هام في الـ security , ألا وهو الـ zoning , والذي يقوم بتقسيم الـ network إلى مجموعة من الـ zones , بحيث كل zone تطبق عليها security level معين وخاص بها, يلائم ويناسب طبيعتها وحساسية الـ devices.

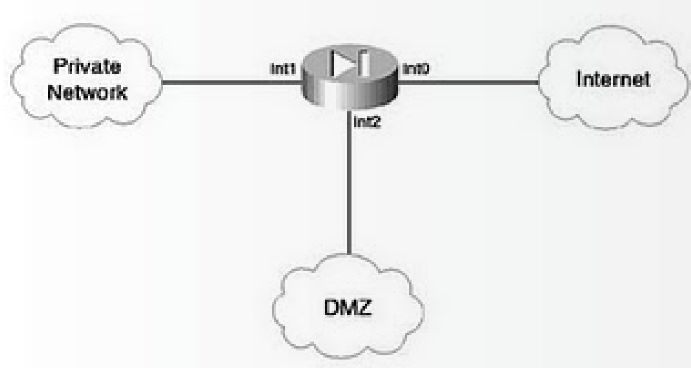
DMZ أو الـ Demilitarized Zone؟

هى عبارة عن zone من ضمن الـ zones (التي سنضعها ببالنا أثناء عملية التقسيم) فهي عبارة عن zone يتم وضعها بين trusted zone و untrusted zone , من المؤكد أنّك ستقول بأنّي شرحت الـ zone , وبأنّي ذكرت نوعين آخرين !, أقول لك نعم, لكنّك مازلت الآن by logic . لو سألتك عن أكثر الأشياء التي تخافها وأنت admin ؟ ستقول النت طبعاً, فمن خلاله يأتي attacks , فبذلك هو أكثر عرضة للـ attacks (بيني وبين نفسي, فإنّي أقول لك إنّي أخاف الناس الذين يقفون إلى جانبك في الشبكة ,) ولو سألتك عن أكثر المناطق التي تعتقد بأنّها آمنة في الـ network ؟ لقلت: الـ local users أو الـ local LAN أنا أثق بأمنها. إذاً ها أنت ذا تقول كلمة « أثق » و التي هي« trusted » هذا معناها ببساطة. الـ net سيبقى untrusted zone بالنسبة لك ,والـ local users بالنسبة لك trusted. حسناً, لقد فهمت هذين الاثنين, لكن هناك الـ DMZ لم تتحدث عنه, كما قلت لك, فهي ستبقى بين الـ trusted والـ untrusted , وهي تمثّل لك خطورة بنسبة ٥٠٪. وما في ذلك ؟ سأقول لك: لو عندك web server أو ftp server سيكون له تعامل كبير مع الـ NET , وبذلك سيمثّل لك نقطة ضعف, وسيتم وضعهم في الـ DMZ .

أنواع الـ DMZ .

هناك أكثر من نوع, وسأشرح ميّزات وعيوب كل واحد منهم, وأترك لك الخيار :

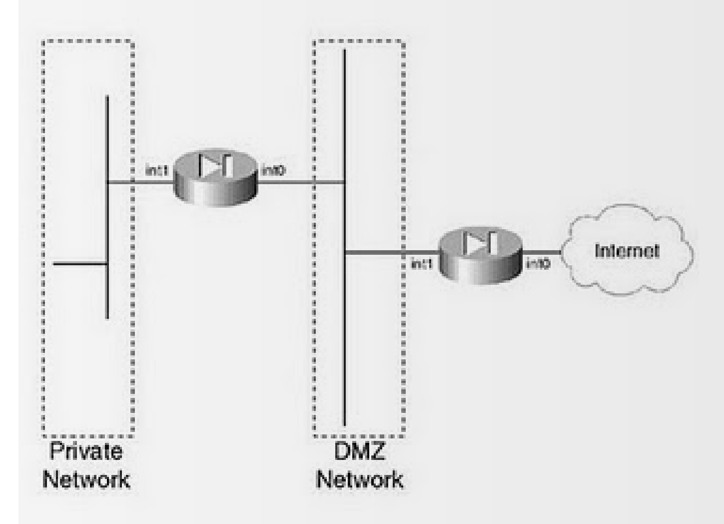
Three-Legged Firewall



سأقوم هنا بتوصيل الـ fire wall , بحيث يكون كل interface مواجه لـ zone معيّنة وعلى حسب درجة الـ security التي أحب أن أطبقها على كل zone من الثلاث , ثم أقوم بعمل الـ configuration على الـ interface عن طريق command في الـ firewall ios يسمى الـ trust level , وهو رقم يتراوح من 0 : 100, أمّا الـ private network سيبقى the more trust , بقي أن أعطيها 100 = trust level , والـ puplic سيعطي الـ interface الموصل به 0 = trust level , وماذا عن الـ dmz ؟ قلنا سابقاً بأنّها ستبقى بين البينيين, بقي مثلاً أن أعطيها قيمة بين الـ 0 والـ 100 وليكن 50 = trust level, من خلال ما تكلمنا عنه وفهمناه عن طريقة الـ configuration نلاحظ

أنّ من ميّزات هذا النوع أنّه easy of configuration وبإمكاننا أيضاً عمل manage للـ network بسهولة. أما العيب في هذا النوع هو لو أنّ الـ network التي لديّ كبيرة جداً و أنا مستخدم هذه الـ topology فإن الـ headace سيبقى عالي جداً على الـ firewall, مما يؤدي إلى استهلاك resources بطريقة فظيعة

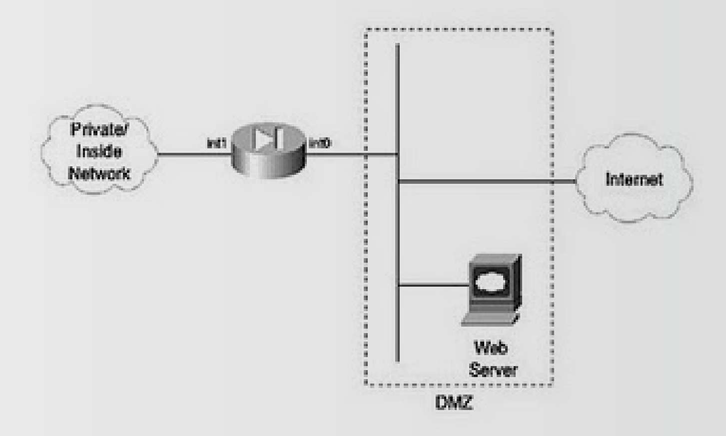
Creating a DMZ Between Stacked Firewalls



في هذا النوع ستمر الـ traffic وهي داخلة أو وهي خارجة على الـ DMZ , ولكن انتبه في حال كانت الـ traffic ضارة فإنّها ستمر على 2 firewalls وهذا يطبق حماية أعلى بكثير من الأنواع الأخرى, ولكن له عيب وهو أن الـ cost سيبقى عالي, ولو قمت بجلب 2 hardware firewalls سيكون تكلفتهم عالية.. وكذلك يفضل أن يكون الـ 2 firewalls من نوعين مختلفين من أجل الـ attacker لو اخترق الأولى لن يجد أي سهولة في اختراق الثانية, أو يستخدم نفس الـ technique التي استخدمها .

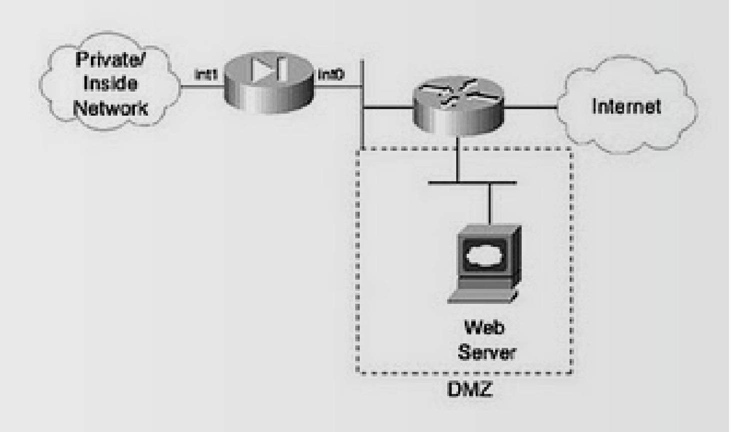


DMZ Outside the Firewall Between the Public Network and the Firewall



في النوع الثاني والذي أعتبره برأيي من أسوأ الأنواع لعمل configuring للـ DMZ . لأنّ الـ traffic القادمة من الـ internet إلى private nw والخارجة من الـ private nw إلى internet يجب أن يكون مرورها من خلال الـ DMZ , وسيكون هذا Not secured بتاتاً .

DMZ Outside the Firewall but not Between the Public Network and the Firewall



هذا النوع هو نفس النوع السابق ولكن الـ DMZ لن تكون الـ traffic الداخلة والخارجة من خلال الـ DMZ, و ستقلل الـ headache الذي كان موجود على الـ firewall كما في الـ three legged .



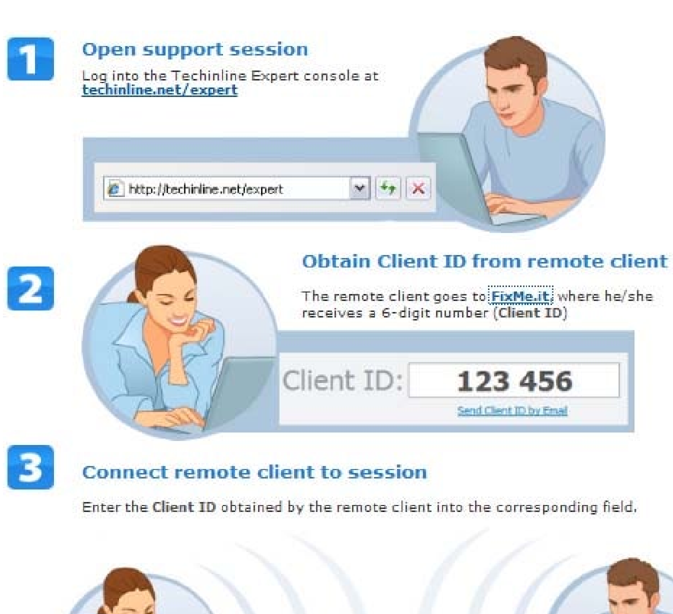
تحكم بسطح المكتب بشكل كامل من خلال متصفح الإنترنت



قررت اليوم الكتابة عن أفضل البرامج المستخدمة في عملية الـ Remote Desktop connection, واخترت أفضل خمس برامج موجودة على الإنترنت, لكن أثناء كتابتي انتبهت أن الموضوع ليس بتلك الأهمية, فجميع البرامج لها نفس المواصفات والإمكانيات باستثناء الأسماء , توقفت عن الكتابة وقررت أن أكتب عن نفس الموضوع لكن بفكرة جديدة لم أجد أحد قد تحدث عنها من قبل وهي Remote Desktop, لكن بدون تنصيب أي برنامج على الجهاز وذلك من خلال المتصفح مباشرة .

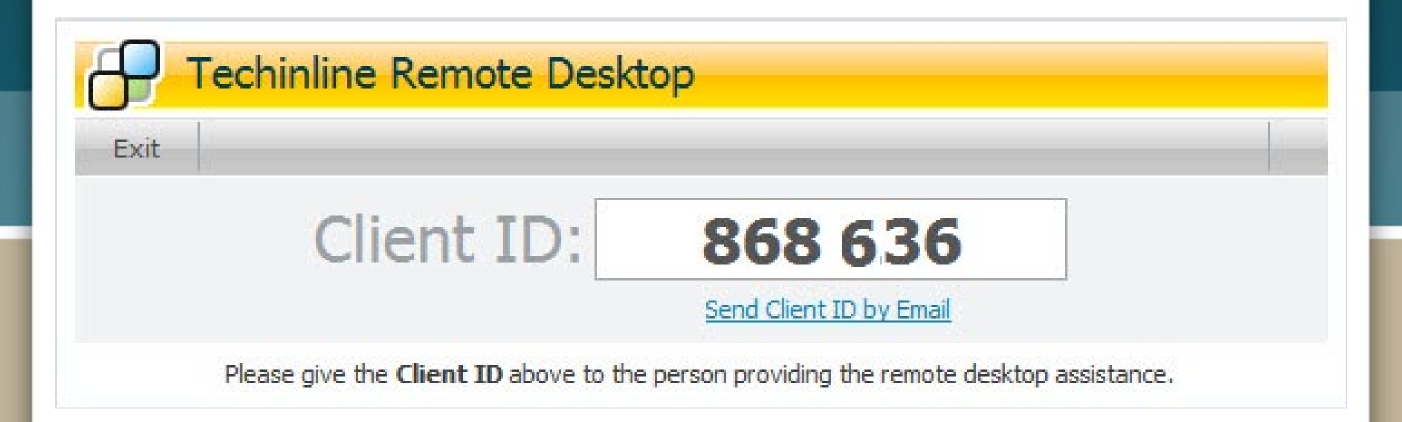
تعتبر برامج الاتصال عن بعد أحد أفضل الحلول المستخدمة في حل المشاكل وإصلاح الأخطاء, ونسبة كبيرة من الناس تستخدم هذه التقنية, لكن كم مرة واجهت صعوبة في شرح كيفية تنصيب البرامج وتشغيلها مع عملائك ؟ بالنسبة لي واجهتني كثيراً, بل وكثيراً جداً, والحل العبقري الذي فكر فيه الغربيون هو في توفير اتصال عن بعد لكن بواسطة المتصفح, بحيث كل الذي عليك فعله هو إضافة Plug للمتصفح لديك فايرفوكس كان أو كروم أو انترنت اكسبلورير, وبعدها أدخل على رابط الموقع وأحصل على رقم خاص بك أو عنوان لكي يتمكن المهندس من الاتصال بجهازك عن بعد .

لنشاهد أولا هذه الصورة التي تشرح كل شيء باختصار .

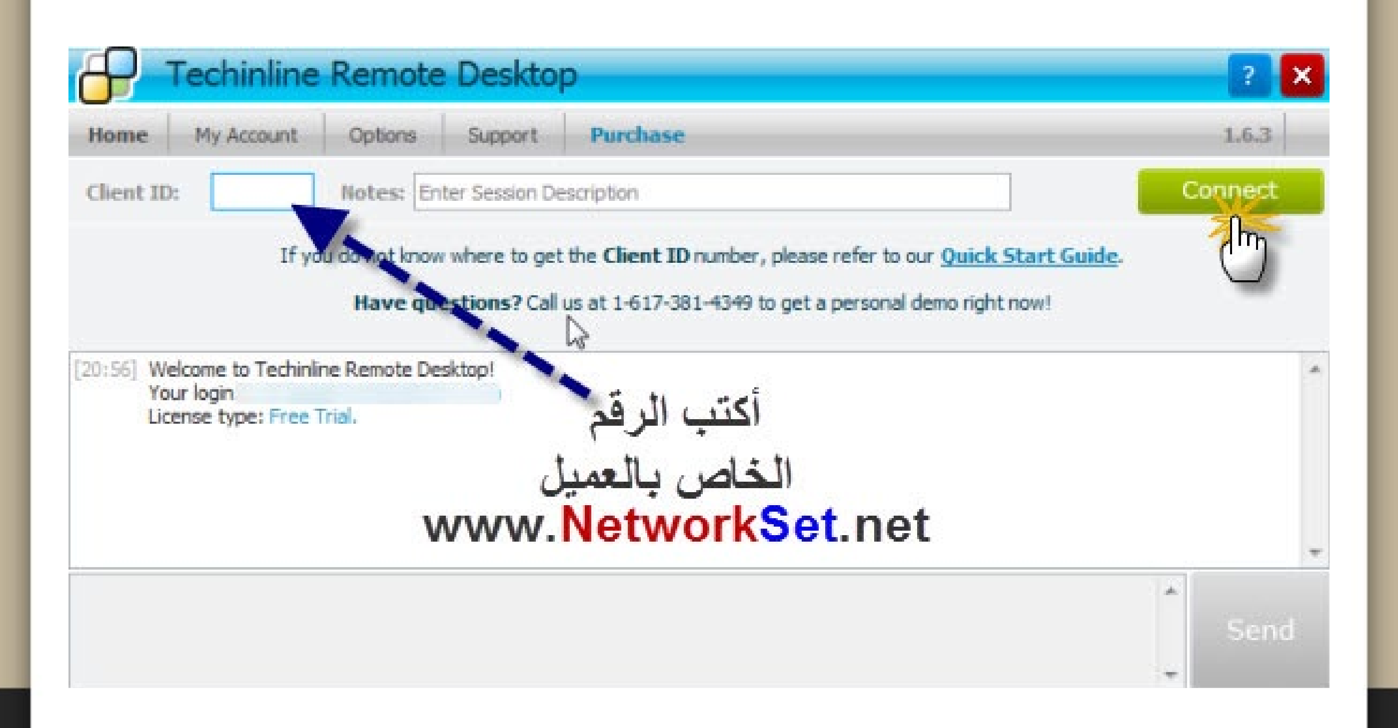


- أولاً: الخبير يقوم بالتسجيل في الموقع من خلال ملئ بعض البيانات مثل الاسم, البريد و إلخ ... وهي للأسف خدمة غير مجانية لكن يمكنك الحصول على 15يوم مجاناً للتجربة, وأعتقد أنّها كافية لحل بعض المشاكل , رابط التسجيل http://www.techinline.com/TryItFree .

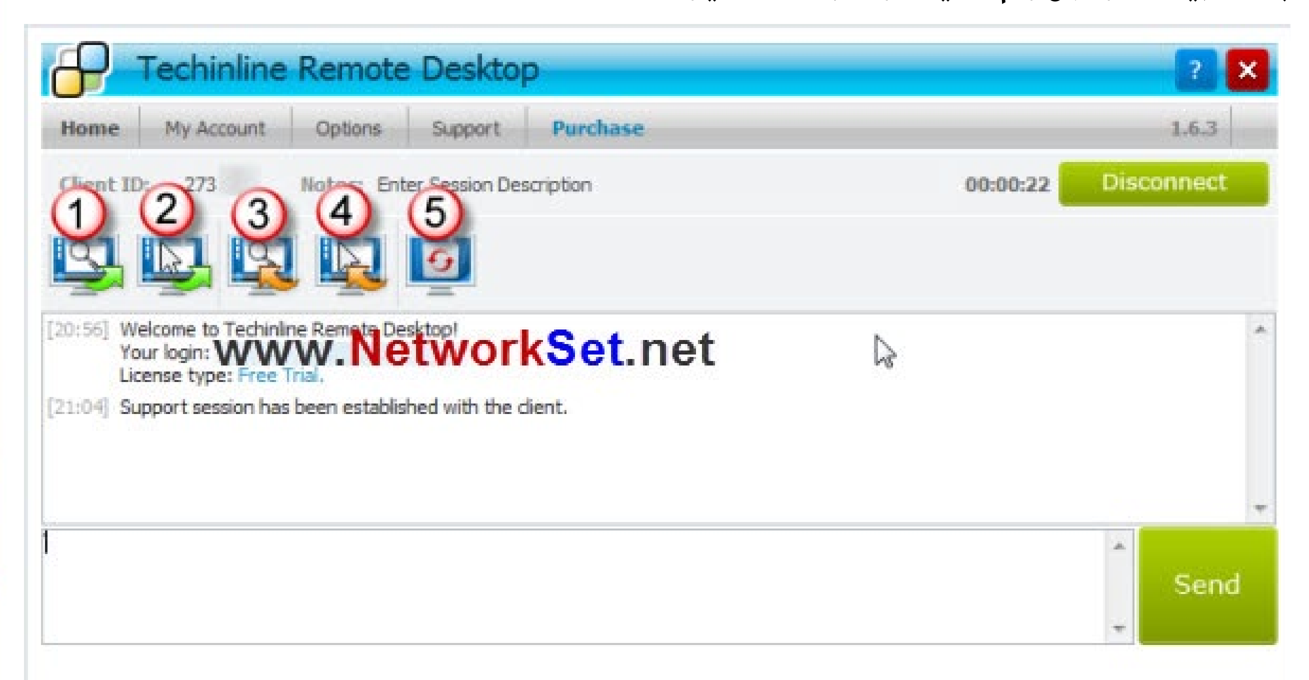
- ثانياً: العميل أو العميلة المبتسمة تتجه إلى موقع fixme.it, وفور الدخول سوف يطالبك الموقع بضرورة تنصيب الـ Plug-in أو extension إلى المتصفح وبغض النظر عن نوعه فهو يدعم كل المتصفحات, وتنصيبه لا يتجاوز الثواني ولا يتطلب منك إلا ضغطة زر واحدة Allow , بالنسبة لي جربته على فايرفوكس وكروم وهو يعمل جيداً , بعد تنصيب الإضافة سوف تحصل على رقم كما هو موضح في الصورة القادمة ومما لاشك فيه أن الرقم يتغير كلما دخلت إلى الموقع , أرسل الرقم إلى الخبير ولا تغلق الصفحة لأنّ طلب الإذن بالدخول سوف يصلك إلى هنا فيما بعد .



- ثالثا: يقوم الخبير بتسجيل الدخول إلى الموقع من خلال الرابط التالي https://techinline.net/expert/ وبعدها يقوم بتسجيل الرقم الخاص بالعميل كما هو موضح, أخيراً اتصال Connect

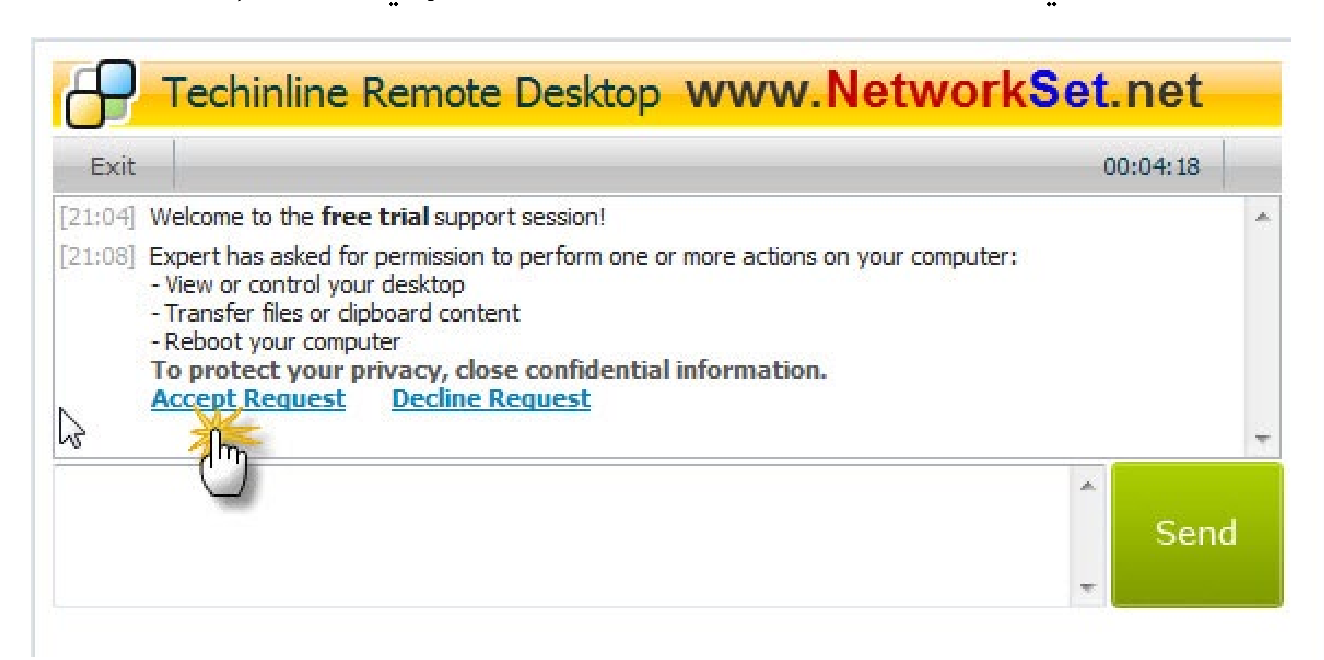


بعد تسجيل الدخول إلى رقم العميل سوف نجد خمسة خيارات



1. مشاهدة سطح مكتب العميل فقط
2. مشاهدة وتحكم بسطح المكتب
3. السماح للعميل بمشاهدة سطح مكتبي
4. السماح للعميل بالمشاهدة والتحكم
5. إغلاق الجلسة أو إعادة الاتصال

سوف أختار الخيار الثاني وأنتظر قليلاً حتى يوافق العميل على الطلب وهو كما موضح في الشكل القادم

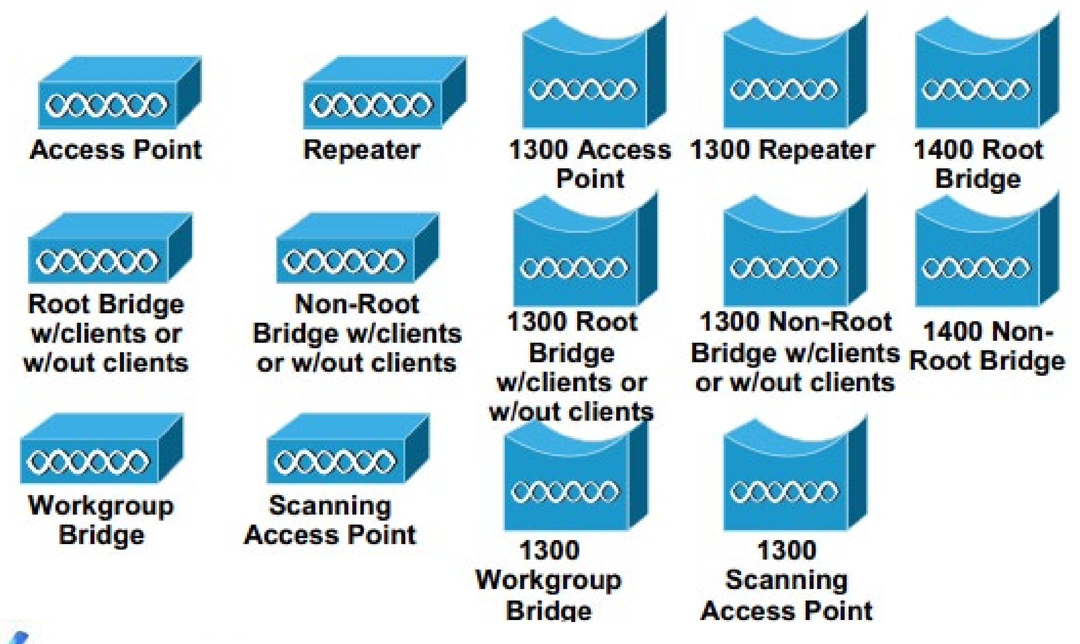


ومع خطوة الموافقة سوف تتمكن من الاتصال عن بعد بالجهاز وسوف تتحكم فيه بشكل كامل مع الكثير من المميزات مثل المحادثة, تبادل الملفات و الخ . . . ولو في حال كنت تملك عضوية مدفوعة فسوف تحصل على مميزات مضاعفة مثل إجراء عدة اتصالات عن بعد في نفس الوقت .





الجسور الّلاسلكية هي أجهزة شبكية تُستخدم غالباً في الشبكات الّلاسلكية الخارجية **Outdoor** , و ذلك للربط بين شبكتين أو أكثر لاسلكياً, حيث يتم الربط على شكل اتصال شبكة بشبكة **Point to point** , أو على شكل اتصال شبكة بعدة شبكات **Point to multipoint**





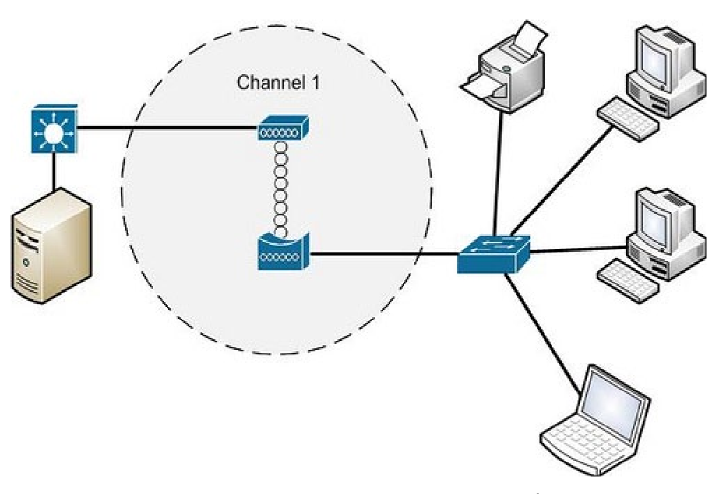
و تعمل الجسور اللاسلكية **Bridges** و الأكسس بوينت على عدة أوضاع, لكل منها استخدامها الخاص, و تسمى هذه الأوضاع في سيسكو بالوظائف الراديوية **Radio Roles** و **Radio Roles** هي الوظائف التي يستطيع أن يقوم بها الجهاز الشبكي اللاسلكي, و هذه الوظائف تختلف من جهاز إلى آخر, و من شركة إلى أخرى, ففي حين تشرح مناهج **CWNP** الوظائف الأساسية فقط, تقوم مناهج **CISCO** الّلاسلكية بالتوسع في شرح هذه الوظائف, وهذا ناشئ عن أن أجهزة سيسكو اللاسلكية قادرة على العمل في وظائف فرعية للشبكة اللاسلكية, سنعرفها الآن بإذن الّله تعالى, و تستطيع اختيار الوظيفة التي تريدها للجهاز من صفحة إعداداته, و هذا مثال من جهاز **BridgeCisco Aironet 1310**

Cisco Systems
Cisco Aironet 1300 Series Wireless Bridge
RADIO0-802.11G STATUS | DETAILED STATUS | SETTINGS | CARRIER BUSY TEST
HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP +
ASSOCIATION +
NETWORK INTERFACES
IP Address
FastEthernet
Radio0-802.11G
SECURITY +
SERVICES +
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +
Hostname 1310 — 1310 uptime is 10 minutes
Network Interfaces: Radio0-802.11G Settings
Enable Radio: Enable / Disable
Current Status (Software/Hardware): Enabled / Up
Role in Radio Network:
Access Point
Repeater
Root Bridge
Non-Root Bridge
Root Bridge with Wireless Clients
Non-Root Bridge with Wireless Clients
Install Automatic
Install Root Bridge
Install Non-Root Bridge
Workgroup Bridge
Scanner

Root access point Role

هنا سيلعب الأكسس بوينت دور الوسيط لتمرير البيانات بين أجهزة الشبكة السلكية وأجهزة الشبكات اللاسلكية و هو الشكل الطبيعي للأكسس بوينت كجهاز اتصال و ربط لاسلكي .

Repeater access point Role

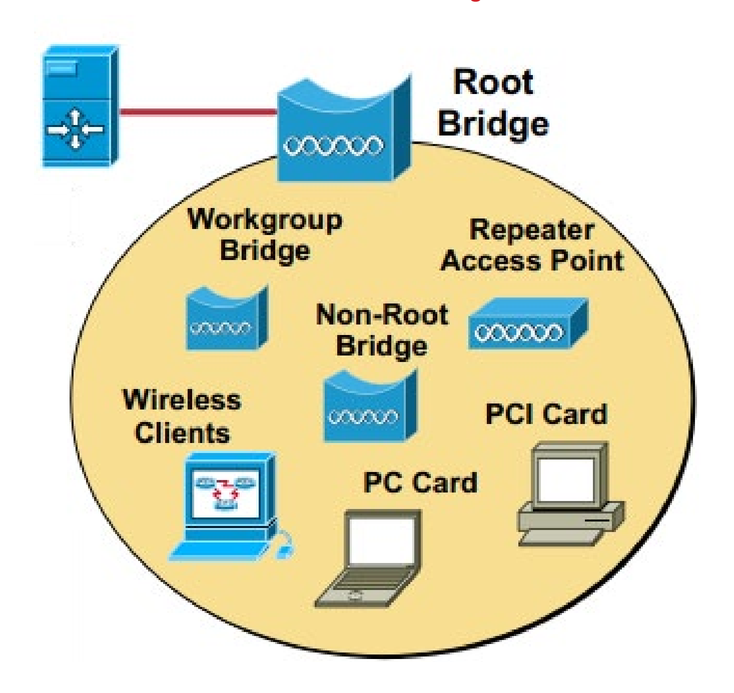


سيلعب هنا الأكسس بوينت دور مقوي الإشارة مع تعطيله لمخارج الإيثرنت في الجهاز, أي أنّه يربط فقط بين الشبكات اللاسلكية

و دور جهاز المقوي أو المكرر Repeater, هو إيصال الإشارة إلى أقصى مكان ممكن أن تصله, ولذلك فإنّ هذا الجهاز يسمى أيضاً بعدة أسماء توحي بطبيعة عمله مثل: wireless range extender و booster و expander فغالب شبكات الوايرلس في العالم تعاني من وجود نقاط ميتة dead zone , و هي مناطق لا تستطيع الأكسس بوينت تغطيتها إمّا لقصور في الأكسس بوينت, أو لبعد هذه المناطق, أو لوجود عوائق تعوق الإشارة.

و لا توجد في سيسكو أجهزة Repeater خاصة و لكن يتم تحويل وضع الأكسس بوينت أو الجسر إلى وضع repeater, أهم شيء لابد أن تفهمه هو أنّ جهاز Repeater ليس جهاز ربط بل مجرد ناقل للإشارة و مقوي لها و أحياناً مقوي لمعدل نقل البيانات Data Rate , و يعمل على نفس قناة الأكسس بوينت الذي يقوي إشارتها

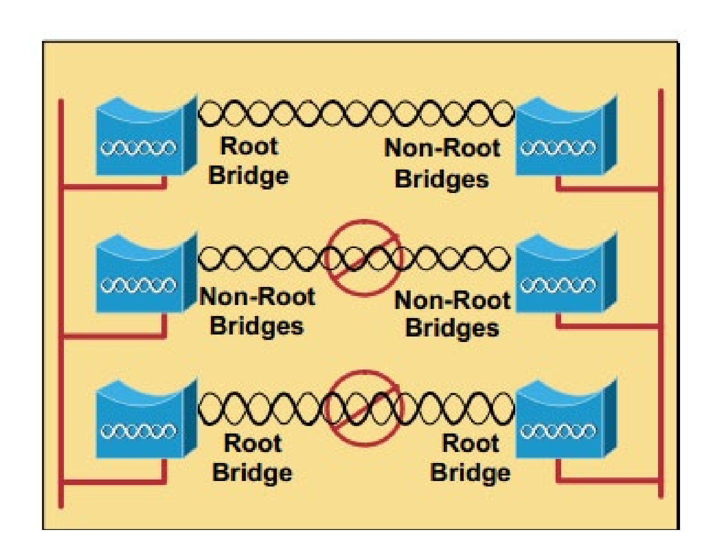
Root bridge with clients Role



هنا سيلعب الجهاز دور الجسر اللّاسلكي الجذري ليربط بين شبكتين لاسلكيتين أو شبكة سلكية و لاسلكية مع إمكانية استخدامه كأكسس بوينت ليسمح للأجهزة بالاتصال به مثل جهاز BridgeCisco Aironet 1310.

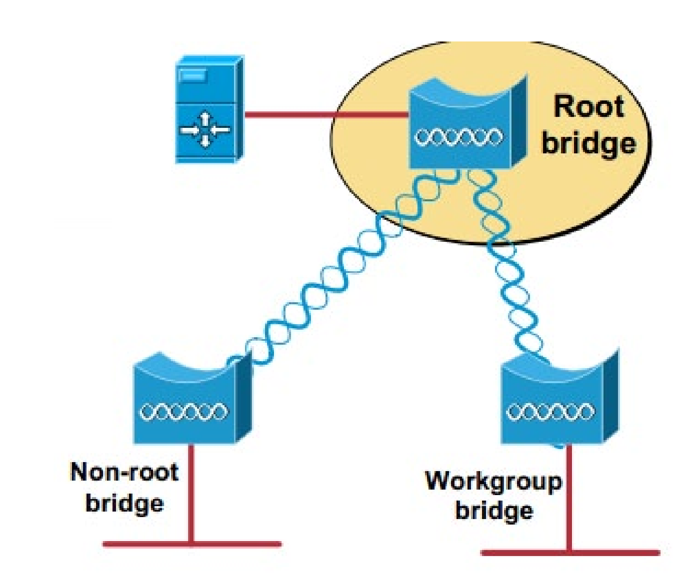
و غالباً Root bridge يكون هو الوضع الافتراضي الذي يأتي

به الجسر, و هو وضع اتصال لاسلكي
للجسر يقوم على أساسه بالاتصال بأجهزة
الجسور الأخرى, شرط أن لا تكون في نفس الوضع,
أي أنّه لا يجوز أن تكون هناك في الشبكة اللّاسلكية الواحدة
سوى جسر واحد فقط في الوضع Root, و يستطيع الجسر
اللّاسلكي في وضع Root الاتصال مع كل الأجهزة اللّاسلكية
عدا الجسور التي تعمل في نفس وضعه و هو Root , كما في
الشكل التالي:



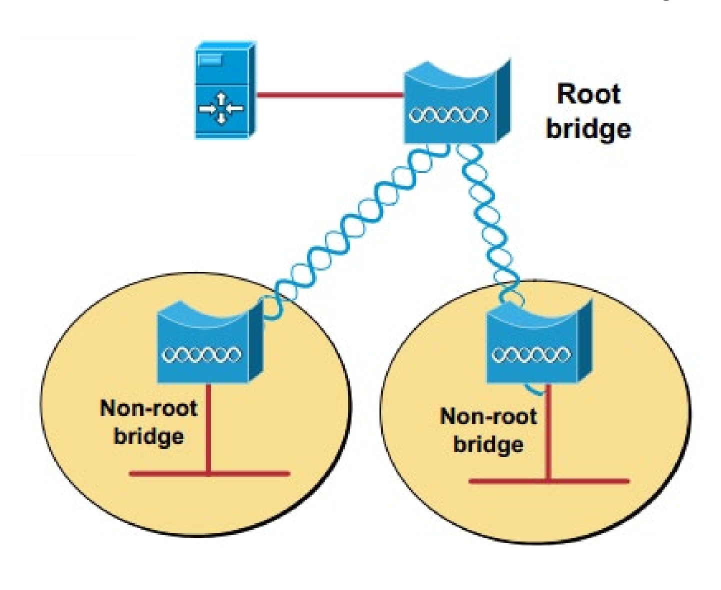
Root bridge without clients Role

لن يتم السماح باتصال العملاء بهذا الجهاز و سيستخدم فقط
كجسر بين الشبكات السلكية أو اللاسلكية, و سيلعب دور
الجهاز الأول أو الجذر في الشبكة اللاسلكية, و لن يسمح لغيره
بهذه الوظيفة مثل جهاز Cisco Aironet 1410 Bridge كما في
الشكل التالي:

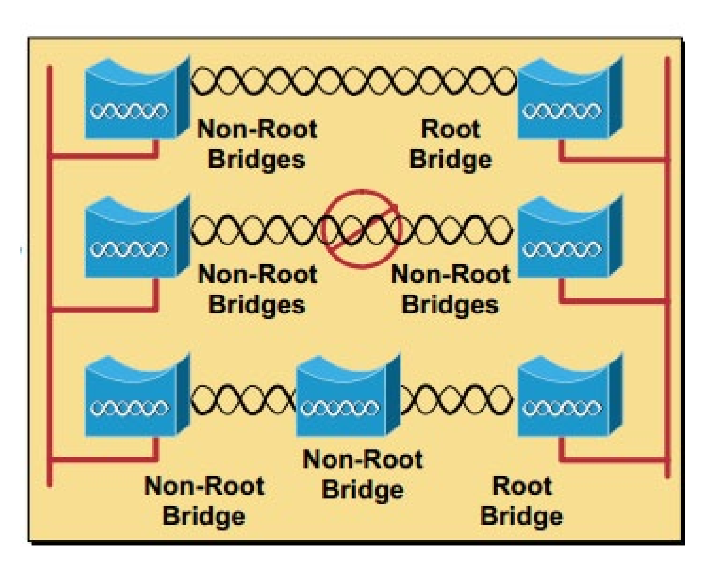


Non-root bridge without clients Role

سيقوم بالاتصال بالجهاز الجذري لينقل الإشارة إلى باقي
الشبكة السلكية أو اللاسلكية, و لا يسمح باتصاله بجهاز آخر
من نفس وظيفته أو عمله كأكسس بوينت مثل أجهزة Cisco
Aironet 1400 Series Bridges



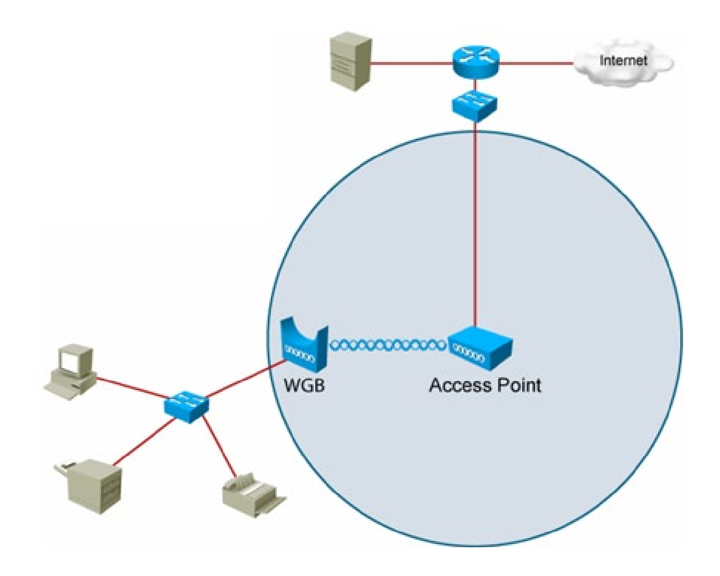
و أجهزة Non-root bridge بشكل عام هي أجهزة الجسور
التي تتصل بالجسر الجذري Root Bridges و لا تستطيع
الاتصال مع مثيلاتها إلّا إذا كان الجهاز Non root الآخر متصل
بجهاز جذري Root Bridge كما في الشكل التالي:



Non-root bridge with clients Role

سيقوم بالاتصال بالجهاز الجذري لينقل الإشارة إلى باقي الشبكة السلكية أو اللاسلكية و لا يسمح باتصاله بجهاز آخر من نفس وظيفته ولكنه سيعمل كأكسس بوينت

WGBWorkgroup bridge Role



هنا سيصبح الجهاز البوابة اللاسلكية للشبكة المحلية السلكية لتتصل بشبكة لاسلكية أخرى, أي كأنّه كارت لاسلكي مشترك للشبكة.

و تتعامل أجهزة الأكسس بوينت مع WGB على أنّه جهاز Client , فلا تستطيع أجهزة الكمبيوتر الاتصال به مباشرة لاسلكيا إطلاقا و لكنه يستطيع الاتصال بأكثر من جهاز أكسس بوينت, و يستطيع أكثر من جهاز WGB الاتصال بأكسس بوينت واحد و لا مجال أيضاً لربط جهاز WGB مع جهاز آخر يعمل في وضع WGB.

لا يقتصر اتصال WGB مع الأكسس بوينت في الوضع الطبيعي لها, بل يستطيع الاتصال بها في وضع المكرر Repeater و يستطيع الاتصال أيضاً بأجهزة الجسور العادية Bridges

Access Point Root (Fallback to Radio Island) Role

سيعمل كجهاز جذري يربط بين شبكتين و سيقوم بالربط اللاسلكي في حال فشل الجهاز في الاتصال سلكيا.

Access Point Root (Fallback to Radio Shutdown) Role

عندما يفقد الجسر اللاسلكي اتصاله بشبكة ما سلكيا, يقوم بقطع الاتصال اللاسلكي عن الأجهزة المتصلة به, و على الأجهزة المتصلة اختيار جهاز آخر للاتصال بالشبكة.

Access Point Root (Fallback to Repeater) Role

عندما يفقد الجسر اللاسلكي اتصاله بشبكة ما سلكيا, يقوم بالتحويل إلى وضع المقوي Repeater

و في النهاية هذه مقارنة بين هذه الأنواع من حيث قابليتها للاتصال ببعضها

	Associates to:				**Accepts Associations from:**			
Role	**Root AP**	**Root BR**	**Repeater AP**	**NR BR with Clients**	**Wireless Clients**	**Wired Clients**	**NR Bridges**	**WGBs**
Root AP				X	X			X
Repeater AP	X	X	X	X	X			X
Root BR			X	X	X	X	X	X
NR BR without Clients		X		X		X	X	
NR BR with Clients		X	X	X	X	X	X	X
Work Group Bridge	X	X	X	X		X		

Real-time Transport Protocol

Identification
فادي أحمد الطه
الجنسية : العراق
مهندس كمبيوتر ومعلوماتية واحضر حاليا لاكمال الدراسات العليا في تخصص شبكات الكمبيوتر. هدفي المساهمة في تطوير العالم
f_altaha88@yahoo.com
IRAQ

عند مشاهدة مقاطع الفيديو الموجودة على الإنترنت, أو سماع المقاطع الصوتية مثل الراديو وغيرها, وكذلك المشاركة في ألعاب الـ online، نحتاج إلى بروتوكول يتحكم بالإرسال والاستقبال ونقل البيانات بشكل فوري, بمعنى آخر تدفق البيانات بصورة مباشرة، لذلك قامت منظمة IETF في عام 1996 بتطوير بروتوكول أطلق عليه Real-time Transport Protocol, أو (RTP) اختصاراً .



في هذا المقال سأقدم مقدمة بسيطة عن هذا البروتوكول، فهو أحد بروتوكولات الطبقة السابعة Application Layer, ومهمته الرئيسية هي نقل بيانات الفيديو والصوت عبر الشبكة, مثل المكالمات الصوتية VOIP, والمؤتمرات الفيديوية video conference, وبث القنوات التلفزيونية عبر الانترنت, وكذلك في الألعاب التي تحتاج إلى نقل البيانات في الزمن الحقيقي, بغض النظر عن دقة البيانات المستلمة كون أن فقدان بعض المعلومات والتي لا يمكن تمييزها خصوصاً عند استعمال خوارزميات معيّنة تكون أفضل من تأخر وصولها كلياً.

فعليّاً, بروتوكول الـ RTP يتكون من جزئين: أحدهما هو البروتوكول نفسه, والجزء الآخر هو بروتوكول RTCP, حيث يعمل جنباً إلى جنب معه. فبينما يعمل بروتوكول RTP على نقل البيانات وترتيبها عند وصولها بتسلسل خاطئ مثلاً، يقوم RTCP بتنظيم هذه العملية عن طريق نقل المعلومات الخاصّة بالتحكم, مثل المزامنة synchronization بين قنوات



النقل المتعددة, ومراقبة عملية QoS المستخدمة لذلك, فكمية المعلومات أو الـ Bandwidth الذي يشغله تساوي 5٪ مقارنة مع الذي يشغله بروتوكول الـ RTP. ويُستعمل بالتوازي مع بروتوكول الـ RTCP بروتوكولات أخرى للتحكم وتنظيم عملية النقل, مثل : RTSP و H.225 وH.245 و SIP.



يتم إرسال البيانات واستقبالها في RTP عبر المنافذ ports الزوجية, بينما في الـ RTCP يتم ذلك عبر المنافذ الفردية التي تليها ومن خلال بروتوكول UDP في الطبقة الرابعة Transport Layer، ومن الممكن أن يكون الإرسال unicast أو Multicast.

من الأشياء الأساسية التي تم أخذها بعين الاعتبار عند تصميم هذا البروتوكول هو دعمه للعديد من الصيغ من ضمنها (H.264, MPEG-4, MJPEG, MPEG), وكذلك يسمح بإضافة صيغ جديدة دون التعديل على البروتوكول، هذا التصميم تم عمله وفقاً للمعمارية التي تسمى ALF)) Application Level Framing.

RTP packet header

يتكون RTP header من 12 بايت على أقل تقدير, ويمكن إضافة عدة bytes إضافية ملحقة بالهيدر، وبعد الهيدر يأتي الـ Payload والذي يُمثّل البيانات.

وبعد أن تعرفنا على حجم الهيدر نأتي الآن لتفصيل أجزاءه:

bit offset	0 - 1	2	3	4 - 7	8	9 - 15	16 - 31
0	Version	P	X	CC	M	PT	Sequence Number
32	Timestamp						
64	SSRC identifier						
96	CSRC identifiers ...						
96 + 32 x CC	Profile-specific extension header ID						Extension header length
128 + 32 x CC	Extension header ...						

Version : ويتكون من 2 bits والذي يحدد نسخة البروتوكول. النسخة الحالية المستخدمة هي الإصدار 2.

P : مختصر Padding, يتكون من 1 بت, ويستخدم لمعرفة ما إذا كان هناك bytes إضافية في نهاية الباكيت المرسلة. هذه الـ bytes تضاف عندما يكون هناك حجم معيّن من الباكيت يتطلب وجوده كقالب عند استعمالها في خوارزميات التشفير مثلاً.

X : مختصر Extension, يتكون من 1 بت, ويستخدم لمعرفة ما إذا كان هناك bytes إضافية ملحقة بالهيدر أم لا, كما ذكرت سابقاً.

CC : مختصر CSRC Count, يتكون من 4 bits, وسيتم ذكر فائدته لاحقاً في CSRC.

M : مختصر Marker, يتكون من 1 بت, ويستخدم لتفعيل خاصيّة تضمين المعلومات الخاصة بحدود الفريم من ضمن الباكيت المرسلة.

PT : مختصر Payload Type, يتكون من 7 bits, ويستخدم لمعرفة صيغة الـPayload وكيفية ترجمة أجزاءه من قِبَل الـ Application Layer .

Sequence Number : يأخذ رقم عشوائي, و يتكون من 16 bits ومن ثم يزداد بمقدار واحد عند كل إرسال ، وعلى الرغم من استخدامه في معرفة ما إذا كان هناك فقد للبيانات أو وصولها بترتيب خاطئ عند المستقبل, إلاّ أنّه عديم الفائدة في هذا البروتوكول, حيث أنّه يترك الأمر للتطبيق المُستَخدَم لتحديد القرار الذي يتطلب اتخاذه. فمثلاً, بعض التطبيقات تقوم بعرض آخِر فريم تم استلامه بدلاً من الفريم المفقود، لهذا فهو يُستعمل فقط لمعرفة ما إذا تم فقد بيانات من عدمها, كونه يعتمد على بروتوكول UDP في عمله.

Timestamp : يتكون من 32 bits, ويستعمل لتفعيل إمكانية عرض الملف بـ Sampling rate معيّن.

SSRC : يتكون من 32 bits, ويحمل رقم عشوائي يُمثّل المصدر المستخدم في المزامنة بين streams.

CSRC : يتكون من 32 bits, ويحدد مصادر البيانات الموجودة في حقل الـ Payload عندما يتم نقل البيانات من أكثر من مصدر. أمّا عدد هذه المصادر والذي يكون 15 كحد أقصى فيتم تحميله في حقل CC.

إلى هنا نأتي إلى نهاية هذه المقدمة السريعة عن هذا البروتوكول ولنا لقاء آخر في مقال آخر إن شاء اللّه.





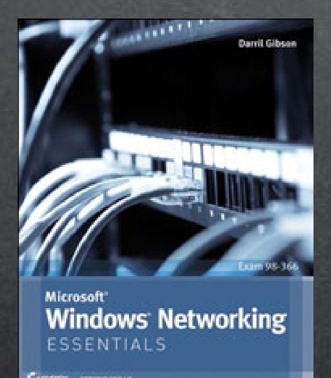
كتاب أعجبني

أحد أكثر المشاكل الشائعة التي مرت علي أثناء تجوالي في المنتديات العربية ، هي أنّ معظم الراغبين في تحضير الشهادات الدولية يعانون من ضعف اللغة الإنجليزية, أو عدم فهمهم السريع عند قراءة الكتب . وهذا ما أشعرهم بالإحباط والتكاسل عن قراءة الكتب الإنجليزية. واكتشفت كذلك أنّ الكثير من الطلاب يستخدم كتب أجنبية ولديه نسخة إلكترونية يقرأها على حاسوبه, ولكن يستحيل أن تجده يقرأ دون أن ترى (ترجمة جوجل) مفتوحة على جهازه . فتراه ليل نهار يترجم فقرة تلو الأخرى, وينتهي من قراءة الكتاب بعد 3 سنوات إن لم نَقُل 300 سنة .

ومن هنا قررت أن أبحث لهذه الفئة من الدارسين عن كتاب يتحدث عن الشبكات بلغة بسيطة مع دعمه للصور, حتى أشجع الدارس العربي على قراءة الكتب الأجنبية, كي ينهي أول كتاب باللغة الإنجليزية مع فهمه, وكذلك ليشجعه على البدء في قراءة الكتب الأجنبية ويبحر في عالم الشبكات .

إسم الكتاب :

Microsoft Windows Networking



الناشر : Sybex

اسم المؤلف :
Darril Gibson

اللّغة : الإنجليزية

عدد الصفحات :
368 صفحة

يتحدث هذا الكتاب بلغة بسيطة جداً عن شبكات ميكروسوفت . فيتطرق بإسلوب بسيط جداً ومدعم بالصور . ففي الفصل الأول يتكلم عن أنواع الشبكات والتقنيات المستخدمة فيها, مع وضع مخطط لكل نوع حتى يسهل على القارئ التفريق بين الأنواع بسهولة . أمّا في الفصل الثاني ، فيتكلم بشكل مختصر جداً عن أجهزة الشبكة وعن أبسط وأهم البروتوكولات, وكذلك يعطي نبذة بسيطة عن أنواع التوبولوجيا . وفي الفصل الثالث ستتعرف على OSI Model, ولكن في هذا الكتاب يعطيك نظرة سريعة فستتعرف على الطبقات وعلى بعض البروتوكولات، وفي أي طبقة تعمل, وكما وسيتطرق أيضاً على TCP/IP Model في هذا الفصل .

أما الفصل الرابع فهو يتكلم عن بروتوكولات TCP/IP . وفي الفصل الخامس والسادس يتكلم عن IPv4 و IPv6, ثم ينتقل بك إلى الفصل السابع والثامن والتاسع ، ليتكلم عن التوصيلات في الشبكة باستخدام الراوترات و السويتشات, ويعطيك فكرة عن العوائق التي تُحدِث مشاكل في التوصيل مثل EMI . وبعد ذلك في الفصل العاشر سيتحدث عن العنونة في الشبكات بشكل عام سواء كانت IP أو Host Name أو DNS . ثم يأتي الفصل الذي بعده ويعطيك نبذة عن الحماية في الشبكات, ويتبعه بالفصل الذي يليه ويعطيك عن أبسط الأشياء التي يجب أن تعرفها عن الشبكات اللّاسلكية . وبعد أن قطعت مشوارك في القراءة ، يأتي الفصل القبل الأخير ويعرّفك بتقنيات الـ WAN ، ثم ينهي الكتاب بفصل مهم جداً للمبتدئين وهو حل وتشخيص مشاكل TCP/IP .

الخلاصة : إذا كنت مبتدأ ولم تقرأ أي كتاب باللغة الإنجليزية في عالم الشبكات ، فهذا الكتاب موجّه لك . أو إذا كنت تريد أن تتسلى وتراجع أبسط أساسيات الشبكات بسرعة فائقة ، فعليك أن تقتني هذا الكتاب .









بروتوكول NTP



ما هي ساعة النظام ؟

إن ساعة النظام هي أهم نقطة في خدمة الوقت ، حيث أنّ ساعة النظام تعمل في اللحظة التي يعمل بها النظام وتتبع باستمرار الوقت والتاريخ الحالي ، ويمكن التحكم بساعة النظام من عدة مصادر ، كما ويمكن أن تستخدم عدة تقنيات لتوزيع الوقت لعدة أنظمة أخرى باستخدام عدة تقنيات أو آليات .



أهمية دقة الوقت في الشبكة

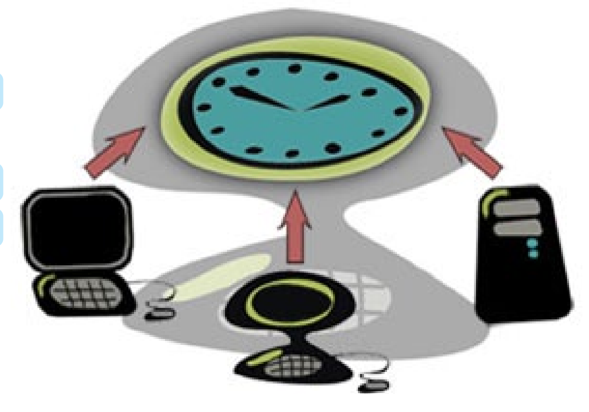
الوقت الصحيح في الشبكة يعتبر مهما لعدة أسباب, حتى أن الثواني أو الأجزاء منها قد تسبب المشاكل في بعض الأحيان ، فعلى سبيل المثال: إن توزيع الإجراءات والمهام يعتمد على الوقت الصحيح للتأكد من إتمامها في الوقت المناسب ، كما أنّ إجراءات الـ Security تعتمد بشكل كبير على الوقت في الشبكة ، وكذلك الكثير من الأمور في حياتنا اليومية كمنظمات أو أفراد تعتمد على الدقة في الوقت, وبالتالي تبرز أهمية استخدام آلية معينة لتنظيم الوقت ومزامنته باستمرار كاستخدام بروتوكول NTP لمزامنة الوقت في أجهزة الشبكة .

كيف تحافظ أجهزة الشبكة على الوقت أثناء إيقاف تشغيلها ؟

إنّ أجهزة الكمبيوتر وبعض أجهزة الشبكة الأخرى تحتوي بداخلها على نظام تقويم يعمل ببطارية يقوم بتتبع الوقت والتاريخ أثناء إيقاف تشغيل هذه الأجهزة ، والتي يمكن إعداد التاريخ والوقت فيها من خلال استخدام بروتوكول NTP .

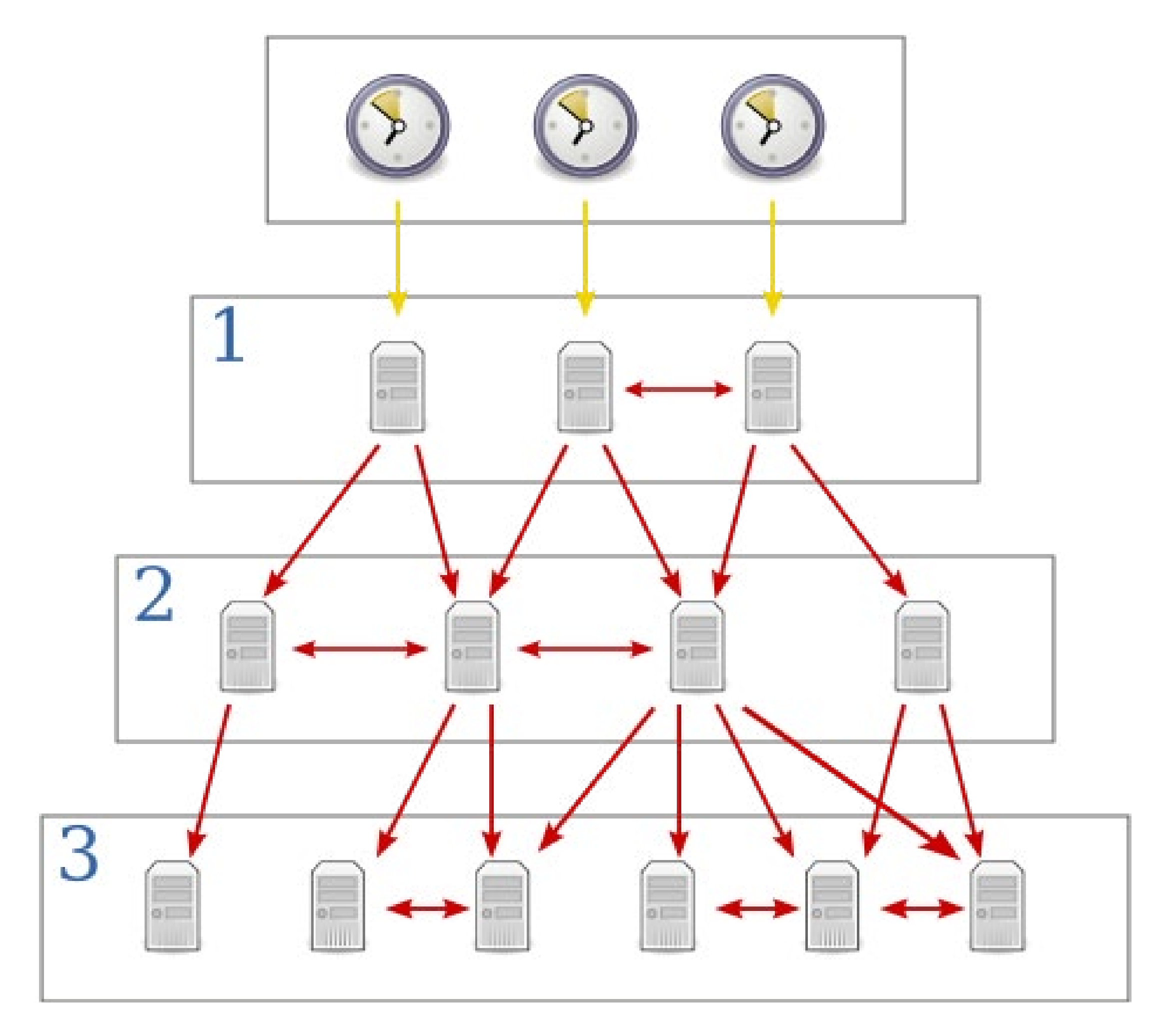
مقدمة عن بروتوكول NTP

NTP هي اختصار لـ Network Time Protocol , وهو بروتوكول تم تصميمه لمزامنة ساعة النظام في أجهزة الشبكة ، حيث قام بتطوير هذا البروتوكول البروفيسور David Mills في جامعة Delaware، ويستخدم هذا البروتوكول بروتوكول UDP من خلال المنفذ 123 في عمليتي الإرسال والاستقبال . الشبكات التي يستخدم فيها بروتوكول NTP تحصل على الوقت من مصادر موثوقة مثل ساعة الراديو والتي تكون موصولة بـ Time Server ، ثم يقوم بروتوكول NTP بتوزيع ذلك الوقت في الشبكة ، وتتم هذه العملية بإنشاء NTP Client, ما يسمى Time Exchange request وإرسالها لـ NTP Server والتي من خلالها يتم ضبط ساعة NTP Client ، وقد يتبادر إلى أذهاننا بأنّ تبادل الرسائل بين الـ Client والـ Server يحتاج لوقت ملموس في بعض الأحيان, خصوصاً عند استخدام شبكة الإنترنت والذي بدوره سيؤثر على دقة الوقت ، ولكن فعلياً فإنّ بروتوكول NTP مصمم لمقاومة العديد من التأخيرات حيث أنّ دقة الوقت عند استخدامه عبر شبكة الإنترنت تصل إلى العشرات من الميلي ثانية, أما عند استخدامه في الشبكة المحلية فإنّ هذه الدقة قد تصل إلى 1 ميلي ثانية .



طبقات الساعة (Clock Strata)

إنّ بروتوكول NTP يستخدم نظام هرمي مقسم لعدة طبقات تعبر عن مستويات من مصادر الوقت ، كل مستوى من هذه المستويات يسمى Stratum ، ويمتلك كل Stratum رقم والذي يبدأ من العدد 0 ويكون في أعلى قمة الهرم ، حيث أنّ مستوى الـ Stratum أو الطبقة يعبر عن بعدها عن الساعة المرجعية ، وهو لا يعبر عن مصداقية الوقت ، ولكن يستخدم لإيجاد مصدر الوقت الخاص بـ Stratum أو بطبقة معينة .



الأسهم باللون لاصفر تشير إلى اتصال مباشر, والأسهم باللون الأحمر تشير إلى اتصال من خلال شبكة .

قد تكون الصورة اتضحت لنا بما تعنيه هذه الطبقات ، ولكن ما هي الأجهزة المستخدمة فعليا في هذه الطبقات ؟ وما هي وظيفتها ؟

: Stratum 0

إنّ الأجهزة التي تمثل هذه الطبقة وكما هو موضح في الشكل السابق هي عبارة عن ساعات مثل ساعات الراديو وساعات الـ GPS ، حيث أنّ هذه الساعات لا تكون موصولة بشبكات ولكن تكون متصلة مباشرة بأجهزة كمبيوتر على سبيل المثال باستخدام -RS 232 .

: Stratum 1

هي عبارة عن أجهزة كمبيوتر تكون متصلة بأجهزة Stratum 0 ، وهي تعمل كخوادم وقت ServersTime لطلب الوقت Timing Requests من خوادم الطبقة Stratum 2 باستخدام بروتوكول NTP ، وتجدر الإشارة إلى وجود أكثر من 300 Server في هذه الطبقة في شبكة الإنترنت .

: Stratum 2

هي عبارة عن أجهزة كمبيوتر تقوم بإرسال طلبات NTP (NTP requests) للخوادم الموجودة في طبقة Stratum 1 ، في العادة إنّ أجهزة الكمبيوتر الموجودة في هذه الطبقة تقوم بالرجوع إلى أكثر من خادم موجود في طبقة Stratum 1 وتستخدم الخوارزمية الخاصة ببروتوكول NTP لاستخلاص أفضل البيانات التي تصلها من خوادم Stratum 1 وتقوم بإهمال الخوادم التي يبدو عليها الخطأ ، كما أنّ أجهزة الكمبيوتر الموجودة في هذه الطبقة تقوم بالاتصال فيما بينها للحصول على وقت أكثر استقرارا لجميع الأجهزة الموجودة في نفس الطبقة ، وهي تعمل كخوادم لطلبات NTP التي تصلها من الطبقة Stratum 3 ، ويوجد في هذه الطبقة في شبكة الإنترنت أكثر من 20,000 Server .

: Stratum 3

إنّ أجهزة الكمبيوتر في هذه الطبقة تقوم بنفس المهمة التي تقوم بها أجهزة Stratum 2 ، وكذلك أيضا يمكنها أن تعمل كخوادم للطبقات الأدنى منها ، ويوجد في هذه الطبقة في شبكة الإنترنت أكثر من 80,000 Server .

نلاحظ مما سبق بأنّ كل طبقة تعمل على خدمة الطبقة الأدنى منها مباشرة كما وأنّها تحصل على وقتها من الطبقة الأعلى منها مباشرة ، كما تجدر الإشارة بأنّ عدد هذه الطبقات في هذا التصميم الهرمي يعتمد على إصدار NTP المستخدم, والذي يمكن أنّ يصل حتى 256 طبقة ، وأن هناك ما يفوق 175,000 مستخدم لبروتوكول NTP في شبكة الإنترنت .

كيف تتم عملية مزامنة الوقت باستخدام بروتوكول NTP ؟

إنّ عملية مزامنة الوقت لدى NTP Client مع NTP Server تتم من خلال عدة عمليات تبادل للبيانات بينهما ، حيث أنّ كل عملية تبادل تتكون من طلب request ورد reply، ولكن الأمر لا يقتصر على ذلك, فإذا دخلت في أعماق هذا البروتوكول أحسست كما لو أنّك في مصنع لديه عدة خطوط إنتاج يقوم بأخذ عينات من كل خط ويدخلها لقسم الجودة لفحصها بعدة مراحل ويقيم جودتها حتى يضمن حصوله على أعلى جودة ممكنة، وهذا يتم في مصنع NTP على النحو التالي :

يقومNTP Clientبإرسال طلب ويقوم بتخزين وقته (originate timestamp) في الـ Packet المرسلة ، وعند استلام NTP Server لهذا الـ Packet يقوم بدوره بتخزين وقته (receive timestamp) فيها ، ويقوم بإرسال الرد بإرجاع الـ Packet إلى الـ Client مع وضع (transmit timestamp) فيها ، والـ Client بدوره عند استلامه للرد يقوم بتسجيل وقت استلامه للـ Packet حتى يقوم باستنتاج الوقت الذي استغرقته الـ Packet أثناء رحلتها .



إنّ الوقت الذي تستغرقه الـ Packet أثناء رحلتها يسمى (delay) ، حيث أنّ هذه الفروقات في الوقت أو هذه المعطيات يمكن استخدامها لاستنتاج الفرق في الوقت بين الجهازين وبالتالي استنتاج الوقت الحالي .

وعلاوة على ذلك, فإنّ هذا الوقت لا يؤخذ بعين الاعتبار حتى تتم عدة عمليات تبادل للـ Packets بين الطرفين ، وكل منها يتم فحصه بمجموعة من الاختبارات ، وإذا نجحت الـ Packets باجتياز الشروط أو الاختبارات الخاصة بالبروتوكول يتم اعتبار الـ Server بأنّه صالح ، أمّا إذا قام البروتوكول باعتبار الـ Server بأنّه غير صالح فإنّه لن يتم مزامنة الوقت مع وقته ، حيث يقوم البروتوكول بوضع بعض القيم التي حصل عليها في فلاتر متعددة المراحل لأغراض إحصائية لتحسين واستنتاج جودة العينات التي حصل عليها من كل Server .

جميع السيرفرات المستخدمة يتم تقييمها لوقت متناسق ، وعند وجود أكثر من سيرفر يوافق عليه البروتوكول والتي تسمى (truechimers) يتم استخدام أكبر عدد ممكن منها في إنتاج مرجع وقت مشترك (combined reference time) ، وبهذه الطريقة يتم إعلان السيرفرات الأخرى بأنّها غير صالحة (falsetickers) .

في الواقع هذه العملية تتطلب 5 دقائق (يتم خلالها معالجة 5 عينات) حتى يتم اختيار NTP Server كمرجع لمزامنة الوقت .
بعد التزامن الأوّلي فإنّ جودة ودقة وقت الـ Client تتحسن مع مرور الوقت ، وبالتالي فإنّه من المحتمل أن يتم اعتبار Server أو أكثر كغير صالحين بعد مرور بعض الوقت .

ما هي إصدارات بروتوكول NTP المستخدمة حالياً ؟

يوجد إصدارين مستخدمين حالياً من بروتوكول NTP وهما NTPv3 و NTPv4 ، بالتأكيد أن الإصدار الرابع أجدد من الإصدار الثالث ، ولكن الإصدار الثالث لا يزال هو المستخدم كمعيار في شبكة الانترنت .

SNTP

يوجد إصدار مبسط من بروتوكول NTP يسمى SNTP وهو اختصار لـ Simple Network Time Protocol وهو إصدار لا يمكن استخدامه إلّا على طرف الـ Client ولا يمكن استخدامه لإرسال الوقت إلى الأنظمة أو الأجهزة الأخرى في الشبكة .

تطبيق بروتوكول NTP في أنظمة تشغيل Microsoft Windows

إنّ نظام تشغيل Windows 2000 وما أنتجته شركة مايكروسوفت من أنظمة تشغيل من بعده تحتوي على خدمة وقت تسمى Windows Time) (Service والتي يمكن أن يتم مزامنة الوقت فيها مع NTP Server ، لكن هذه الخدمة في Windows 2000تحتوي على ميزات SNTP فقط, وهي تخرق المقياس NTPv3 من عدة جوانب .

منذ إصدار Windows Server 2003 بالرغم من أن خدمة Windows Time لم تكن تطبيقا دقيقا لبروتوكول NTP ، إلّا أنّها تستخدم مجموعة معقدة من الخوارزميات المستخدمة في بروتوكول NTP للتأكد من دقة ساعات النظام في أجهزة الكمبيوتر في الشبكة قدر الإمكان ، ولكن بالرغم من ذلك فإنّ خدمة Windows Time لا تستطيع توفير دقة في الوقت لأكثر مما يقارب ثانية أو اثنتين .

المراجع :
http://www.cisco.com
http://networking.ringofsaturn.com
http://www.ntp.org
http://en.wikipedia.org
http://www.microsoft.com



تتقدم إدارة موقع

NetworkSet

First Arabic Magazine for Networks

بالشكر والتقدير للمهندس الفلسطيني

أحمد غزال

تقديرا لتفاعله ومشاركته الكبيرة معنا في قسم الأسئلة والأجوبة
بارك الله فيه وفي وقته الذي منحه لأخوانه .

مؤسس ومدير موقع NetworkSet
المهندس أيمن النعيمي

2011 / 12 / 25

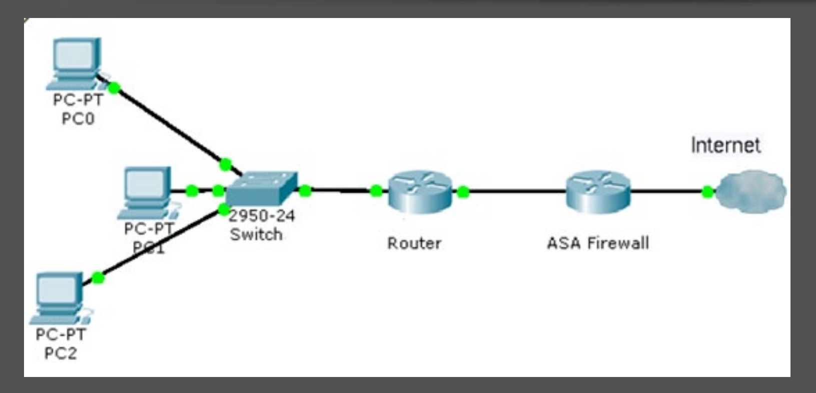
NetworkSet
First Arabic Magazine for Networks
المجلة العربية المتخصصة بالشبكات



كيف تحمي شبكتك

من الضروري لمهندس الشبكات أن يكون مُلِم ببعض التقنيات و الاستراتيجيات المهمة التي تُستخدم في صد الهجمات وأشهر الطرق التي من الممكن أن يتّبعها للتعرف على نوع الهجمات الموجهة إلى شبكته. خلال هذا المقال سنتعرف على عدد من هجمات الشبكة و كيف يتصرف الشخص المسؤول عنها في حال استُهدِفت الشبكة بهجوم معين .

* شكل الشبكة التي سنعتمد عليها في الشرح



التصدي لهجمات الـ Fragmentation-Based Attack

عدد كبير من الهجمات تعتمد على عملية الـ Fragmentation, أي تقسيم الـ Packets إلى أجزاء صغيرة يتم إرسالها بشكل متتابع فيتم تجميعها مرة أخرى , بعض البرامج يمكنها استغلال بعض الثغرات في هذه العملية لتنفيذ غرض خبيث في نظام التشغيل أو حملها إلى بعض التصرفات الغير محسوبة مما يؤدي إلى حدوث خلل, يمكن أيضاً استخدام الـ Fragmentation بغرض إخفاء هجوم كبير يتم تنفيذه, فعن طريق الـ Fragmentation يتمكن المخترق من المرور عبر أنظمة الحماية مثل الـ IPS و الـ IDS وبعض الجدران النارية, باختصار الـ Fragmentation يمكن أن يؤدي إلى الكثير من المشاكل و الثغرات, مثال على أشهر الطرق الخبيثة التي تعتمد على الـ Fragmentation في تنفيذ شيء معين :

- IP fragment overlapped
- IP fragmentation buffer full
- IP fragment overrun
- IP fragment overwrite
- IP fragment too many datagrams
- IP fragment incomplete datagram
- IP fragment too small

بما أن الهدف من المقال هو طريقة الحماية فلن أتطرق إلى الحديث عن هذه الطرق , في حال أنّه تم إخبارك أنّ هناك من يعتمد على هذه الطرق لعمل خبيث و طلب منك منع ذلك فالأمر بسيط, كل ما عليك فعله هو تنفيذ إحدى هذه الطرق الآتية :

1.الطريقة الأولى: عن طريق الـ Router

```
R1(config)#access-list 101 deny ip any
any fragments

R1(config)#access-list 101 permit ip any
any

R1(config)#interface f01/

R1(config-if)#ip access-group 101 in

Router(DDNS-HTTP)#exit

Router(DDNS-update-method)#interval
maximum 14 0 0 0
Router(DDNS-update-method)#exit
```

عن طريق الأوامر السابقة تم إنشاء ACL تقوم بمنع أي fragment من المرور عن طريق الـ keyword التي أضفناها في نهاية الأمر fragments, وهي تقوم بعمل match لل Non Initial Fragments, ولكن ما الفرق بين الـ Initial fragment والـ Non Initial fragments ؟

- الـ fragments Initial هي التي تحتوي على كل القيم المطلوبة والمهمة في الـ Headers , فهي تحتوي على Layer 3 &4 Information وبهذا يمكن للـ ACL العادية التعرف عليها .
- الـ fragments Non Intial هي التي لا تحتوي على معلومات كافيه في الـ Header وفي الغالب لا تحتوي على أي

معلومات خاصة بـ Layer 4 , لذلك لا يمكن لـ ACL العادية التعرف عليها إلّا عن طريق كلمة fragments .

2.الطريقة الثانية: عن طريق الـ Router

```
R4(config)#int fa01/
R4(config-if)#ip virtual-reassembly
drop-fragments
```

هذه الطريقة تعتمد على خاصية تسمى Virtual-reassembly ,وظيفة هذه الخاصية في الأصل أنّها تقوم بتجميع كل الـ Fragments على شكل Packet واحد, فيستطيع الـ Router عمل Inspect لها في حال إذا كان الروتر يعمل كجدار ناري, ولكننا هنا استخدمنا هذه الخاصية لمنع الـ Fragments بشكل نهائي .

3.الطريقة الثالثة: عن طريق ASA

```
ASA(config)# fragment chain 1 outside
```

الأمر السابق يقوم بتحديد أكبر عدد من الـ Fragment يمكن السماح به لـ Packet الواحدة , وبما أنّنا قمنا بجعل هذه القيمة تساوى 1 فيما معناه «لا تسمح بمرور أكثر من Fragmnet واحدة لكل Packet», أي أنّنا بهذا قمنا بمنع الـ Fragmentation .

التصدي لهجمات IP Options-Based Attack

فى كل IP Header يكون هناك خاص بالـ IP options ويكون بعد الـ Destination IP address , وهذه صورة لـ Header للتوضيح

Version	Header	Type of Service	Total Packet Length (in Bytes)			
Identification			O	D	M	Fragment Offset
Time to Live (TTL)	Protocol		Header Checksum			
Source Address						
Destination Address						
Options						
Payload						

في أغلب الاتصالات يكون هذا الجزء فارغ, فهو يستخدم في حالات قليلة مثل رسائل الـ BGP التي تستخدم IP option 19, لكن هناك بعض الاستخدامات الخبيثة في هذه الجزئية تُمكِّن المخرب من عمل Spoof وأشياء أخرى, ولمنع حدوث ذلك يمكنك استخدام الطريقة التالية :

```
R1(config)#ip options drop
```

هذا الأمر يقوم بعمل Drop لهذا الـ Traffic .

التصدي لهجمات الاستطلاع Reconnaissance

أي عملية اختراق منظمة تبدأ بهذه الخطوة, و هي تساعد في معرفة معلومات عن الشبكة مثل نطاق العناوين المستخدم والمنافذ المفتوحة إلخ... من هذه الأمور ,من أشهر البرامج التي تقوم بهذه العملية البرنامج الشهير nmap . إذا كنت تشك أن هناك من يقوم باستطلاع شبكتك فقم بإدخال هذا الأمر في الـ ASA

```
ASA(config)# threat-detection scanning-
threat shun duration 1800
```

خاصية Threat-detection هي خاصية مهمة في الـ ASA لها استخدامات عديدة , هذا الأمر لا يقوم بمنع أي استطلاع على الشبكة فقط , بل يقوم بعمل block لأي جهاز يصدر منه هذا النشاط لمدة معينة من الثواني تقوم أنت بتحديدها. ملحوظة مهمة للحماية من هجمات الاستطلاع وهي أن لا تسمح بأكثر مما تحتاجه الشبكة للعمل بالمرور, فإذا سمحت بأكثر من ذلك ستجد الباب مفتوح للعديد من الهجمات, فمثلاً إذا كان عندك HTTP سيرفر تسمح لأي شخص من الإنترنت بالولوج إليه, فلا تستخدم الـ ACL على الإنترفيس المواجه للإنترنت بهذه الطريقة

```
access-list 101 permit tcp any any eq
80
```

بل اجعلها بهذه الطريقة لأنّها أكثر أمناً

```
access-list 101 permit tcp any SERVER-
IP eq 80
```

التصدي لهجمات التزوير IP Spoofing

فى الغالب يلجأ المخربين إلى تزوير عناوين الـ IP الخاصة بهم سواء من أجل التخفي أو أي غرض آخر. من مبادئ الحماية أن لا تسمح مطلقاً بأي عنوان ضمن RFC1819 بالدخول إلى شبكتك عن طريق الإنترنت, لأن هذه العناوين خاصة بالـ Private Host, لذلك إذا كان مصدرها الـ Outside فحتماً ولابد أنّها عناوين غير حقيقية, لذلك يُفضّل أن يكون الإنترفيس المواجه للإنترنت عليه ACL بهذا الشكل

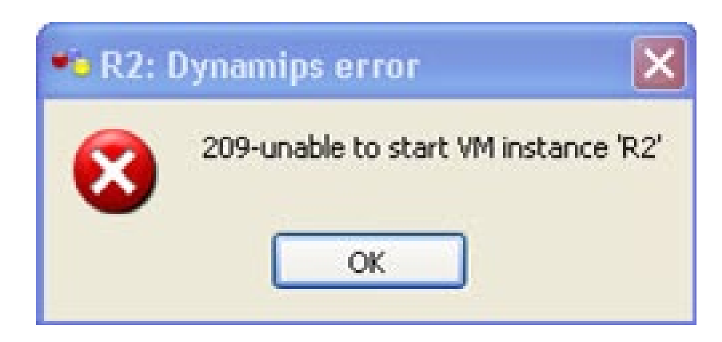
```
R1(config)#access-list 101 deny ip
192.168.0.0 0.0.255.255 any
R1(config)#access-list 101 deny ip
172.16.0.0 0.15.255.255 any
R1(config)#access-list 101 deny ip
10.0.0.0 0.255.255.255 any
R1(config)#access-list 101 permit ip any
any
```

بهذا أكون قد انتهيت وأتمنى أن يكون المقال سهل و مفهوم , ومازال هناك الكثير من طرق الحماية, نتعرف عليها في العدد القادم .



GNS3 Error 209

'209-unable to start VM instance 'R



كثيراً ما تظهر هذه الرسالة للمبتدئين عند استخدام الـ GNS3، وبعدها يتوقف البرنامج ولا تستطيع تشغيل الراوتر مثلاً، وهذه الـ Error رقم 209 يمكن تقسيم أسباب حدوثها إلى سببين:

1 - وجود حروف أو كلمات غير اللغة الإنجليزية"ASCII" مثل حروف اللغة العربية مثلاً أو اللغة الصينية أو ما يطلق عليه "UNICODE" في اسم الملف الموجود فيه نسخ الـIOS:

«American Standard Code for Information Interchange : ASCII»

«"Unicode : Universal Code

IOS image	Model/Chassis
127.0.0.1:C:\Documents and Settings\Administrator\My Documents\IOS\C2600-AD.BIN	2621
127.0.0.1:C:\Documents and Settings\Administrator\My Documents\IOS\C2691-AD.BIN	2691
127.0.0.1:C:\Documents and Settings\Administrator\My Documents\IOS\C3640-IK.BIN	3640
127.0.0.1:C:\Documents and Settings\Administrator\My Documents\IOS\C7200-AD.BIN	7200
127.0.0.1:C:\Documents and Settings\Administrator\My Documents\IOS\c3725-adventerprisek9-mz.124-15.T5.bin	3725
127.0.0.1:C:\Documents and Settings\Administrator\My Documents\سيسكو\C1700-AD.bin	1710

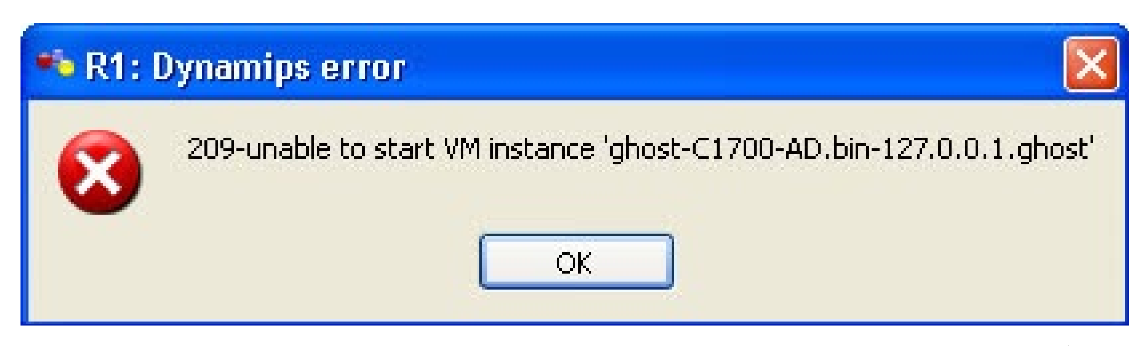
فكما نلاحظ في الصورة السابقة أنّ السطر الأخير والذي يشير إلى مكان وجود نسخ الـ IOS على الجهاز مكتوب باللغة العربية «سيسكو». مع ملاحظة أنّ الرموز الخاصة مثل # $ ٪ @ وغيرها لا تؤدي إلى ظهور هذا الخطأ في حالة وجودها في اسم الملف.

وبدءً من النسخة 0.7.3 بدأ البرنامج في إظهار رسالة وجود حروف الـ UNICODE في اسم الملف وذلك لتفادي حدوث هذا الخطأ:



ولكن على الرغم من ذلك، في حالة الضغط على OK فإنّ البرنامج سوف يقوم بإدراج النسخة بالرغم من وجود حروف الـ UNICODE في اسم الملف.

2 - أحياناً تظهر رسالة الخطأ السابقة بصيغة مختلفة:



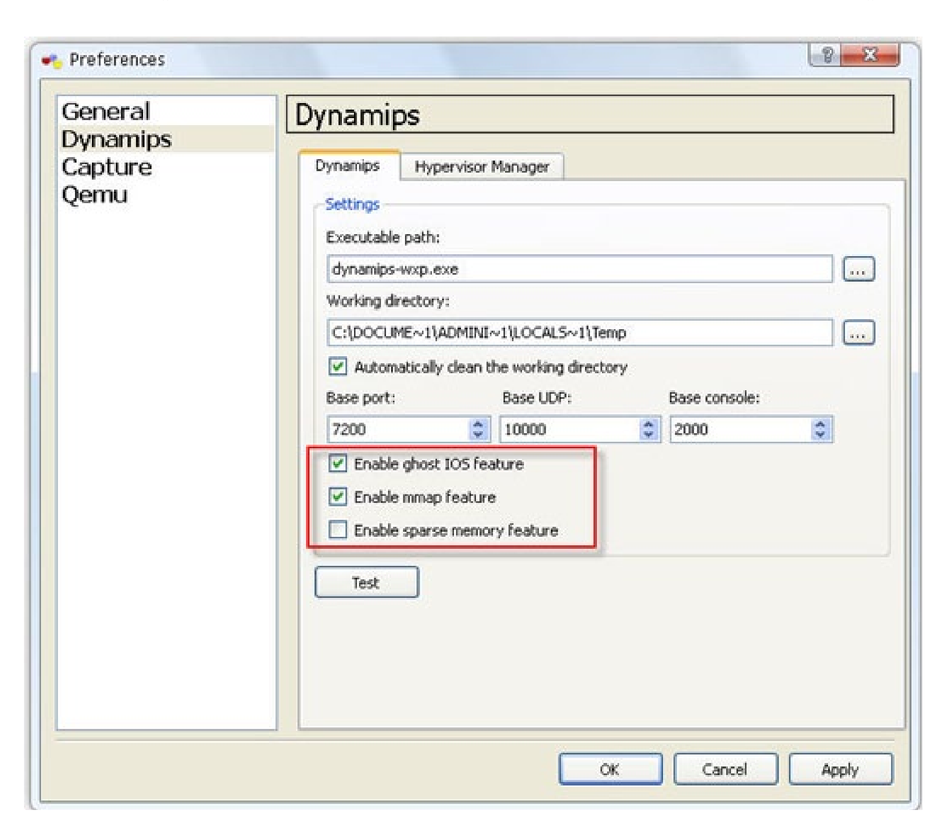
وهذا ليس عائداً لوجود حروف الـ UNICODE كما أسلفنا، ولكن بسبب الـ ghost ios.

الجديد في الرسالة هو الـ ghost ios، فما هو؟

حينما تقوم بتشغيل عدة راوترات من نفس النوع ولنقل مثلاً 3640 -وهي أخف نسخة على الجهاز-، فبدلاً من أن يقوم كل راوتر على حدا بتخزين نسخة من الـ IOS المستخدمة في الـ «virtual RAM» الخاصة به، -وبالتالي مع زيادة عدد الراوترات تزيد نسبة الـ«virtual RAM» المستخدمة بصورة كبيرة- يقوم البرنامج بعمل «shared memory» لجميع الراوترات المستخدمة في اللاب بشرط أن تكون جميع الراوترات من نفس النوع.

فمثلاً إذا كان لدينا 10 راوترات من نفس النوع وحجم كل واحد 50 ميجابايت، هنا نلاحظ أنّنا نحتاج إلى 500 ميجابايت من «real RAM» لهذه الراوترات مع ملاحظة بطء شديد في الجهاز عند محاولة تشغيل العشر راوترات في نفس الوقت، ولكن مع خاصية الـ ghost ios، يقوم البرنامج باستخدام 50 ميجابايت فقط من الـ«real RAM» لأنّه يستخدم نفس نسخة الـ IOS لجميع الراوترات المستخدمة.

كيف يتم تفعيل هذه الخاصية؟
هذه الخاصية مفعّلة في برنامج الـ GNS3 وذلك «By Default» ونلاحظ ذلك كما في الصورة التالية :



ولكن نلاحظ أنّ هذه الخاصية غير مفعّلة في الوضع الافتراضي «Defualt» في برنامج الـ Dynagen،والسبب في ذلك أنّك تقوم بكتابة جميع الجمل في ملف الـ«.net»، لذلك نقوم بتفعيلها باستخدام الجملة التالية

```
ghostios = true
```

ولحل هذه المشكلة هناك طريقتين:

١- عن طريق عدم تفعيل خاصية الـ ghost ios من خلال الـ GUI كما في الصورة السابقة، بعدم اختيارها، وهذا سوف ينطبق على جميع اللابات اللاحقة وبذلك نفقد فوائد الـ ghost ios.
٢- عن طريق فتح ملف اللاب .net file وإعطاء الـ ghost ios القيمة false بدلاً من true، وذلك لكل راوتر، في حالة استخدام أكثر من نسخة مختلفة من الـ IOS، بمعنى آخر موديلات مختلفة من الراوترات، كالتالي:

```
autostart = False
[localhost:7200]
workingdir = EXAMPLE_working
udp = 10000
    [[3725]]
        image = C:\Documents and Settings\Administrator\My Documents\ios\
c3725-adventerprisek9-mz.12415-.T5.bin
        ram = 128
ghostios = false
idlepc = 0x60bedba0
    [[7200]]
        image = C:\Documents and Settings\Administrator\My Documents\ios\
C7200-AD.BIN
idlepc = 0x8046b800
ghostios = false
    [[3640]]
        image = C:\Documents and Settings\Administrator\My Documents\ios\
C3640-IK.BIN
idlepc = 0x60618538
ghostios = false
        chassis = 3640
```

سيرفر المايكروتك (نظرة عن قرب)





هل تسائلت يوماً ما عن التحكم بخدمة الإنترنت عن طريق الويندوز سيرفر ؟

هل لديك مستخدمين على شبكة الإنترنت الخاصة بك ؟ و بسبب قيامهم بعمليات تنزيل البيانات ليل نهار, أدى ذلك رفع ضغطك وانزعاجك من ثم إلى بطء السرعة في الشبكة ؟

هل واجهت يوماً ما مشكلة في سيرفر المايكروتك ولجأت لأحد مهندسي الأنظمة ليساعدك, وصدمت عندما قال لك :

«لم أسمع بهذا السيرفر في حياتي !!»

من هنا كان سبب كتابتي لهذا المقال ، وهو أنّ الكثير منّا لا يعرف ما قيمة هذا السيرفر أو أنّه لم يسمع به أبداً . أمّا السبب الثاني, هو أنّ معظم المؤسسات تعتمد على الويندوز سيرفر, وأنّ مهندسيها يبحثون دوماً عن خيارات تساعدهم في التحكم بخدمة الإنترنت بشكل كامل, في حين يأسوا من عدم تمكنهم من ذلك .

في هذا المقال سنتطرق لأهم الأمور الأساسية التي يقدمها سيرفر المايكروتك والتي يحتاج لمعرفتها المستخدم.

ما هو سيرفر المايكروتك ؟

هو سيرفر أنتجته شركة المايكروتك والتي تأسست 1995 . ويُستخدم هذا السيرفر لإدارة خدمة الإنترنت فقط . لذلك يستخدم غالباً في الشبكات التجارية . ويمكنك الحصول عليه كسوفت وير أو هاردوير, والذي يأتي مع RouterBoard المستخدمة في الشبكات اللاسلكية لتعمل كـ Access Point أو Bridgeوالموضحة في الصورة التالية :



والجدير بالذكر هنا ، هو أنّ هذا السيرفر يأتي بعدة مستويات وتكون من المستوى 1 إلى 6 . ويتميّز كل مستوى بخصائص, ومن أهمها عدد المستخدمين, والذي يستطيع السيرفر استقبالهم للعمل في نفس الوقت بالإضافة إلى عدد المستخدمين في الـ User Manager, وهي الميّزة التي تدير المستخدمين بشكل منتظم وتلقائي, كأن نقطع الخدمة على مُستخدم (كل يوم ثلاثاء من كل أسبوع) .

فمثلاً الإصدارات التي تعمل على level 6 عدد مستخدميها غير محدود, في حين يكون عدد المستخدمين في level 5 والذين استخدموا الخدمة في نفس الوقت (500 مستخدم), وعدد المستخدمين الممكن إضافتهم في الـ User Manager (50 مستخدم) . خلاصة الكلام نقول: بأنّ المستويات فقط تحدد الحد المعيّن لعدد الخدمات, أمّا بقية الميّزات فهي متوفرة في كل مستوى والتعامل مع السيرفر نفسه في كل مستوى .

ما هي متطلبات تنصيب سيرفر المايكروتك ؟

إمّا أن تشتري RouterBoard ويكون نظام السيرفر مركب عليها, أو تشتري نسخة من السيرفر كسوفت وير تركبها على جهاز الكمبيوتر . ولتركيب النسخة على جهاز كمبيوتر ، فإنّ أقل مواصفات ينصح بها هي كالتالي :

Processor : Pentium 4 , 2.0GHz
RAM : 512MB
Hard Disk : 40GB

هذه المواصفات لشبكة تحتوي على عدد لا يتجاوز 20 مستخدم . أمّا الشبكات الضخمة فإنّها بحاجة لمواصفات عالية.

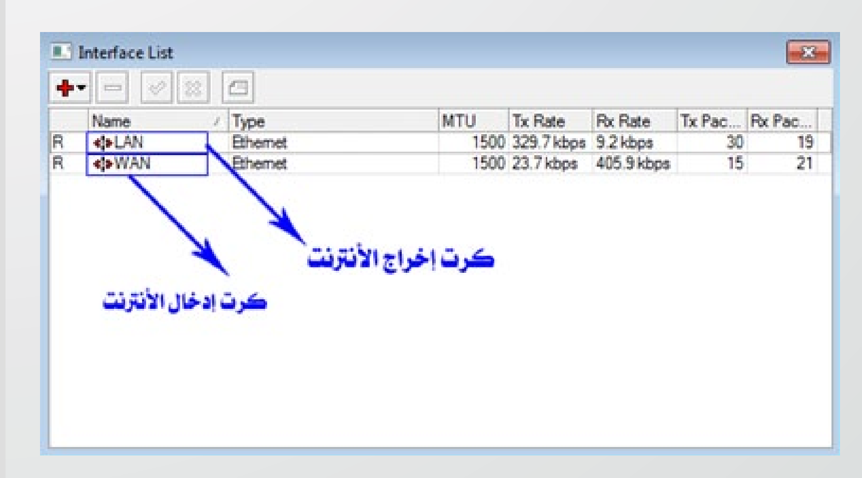
ما هي إمكانيات ومميزات هذا السيرفر ؟

ما يجب عليك أن تضعه بعين الاعتبار ، هو أنّ هذا السيرفر يُستخدم لإدارة خدمة الإنترنت في الشبكة فقط . فهو يُزودك بإمكانيات كثيرة جداً, وسنتطرق لأهم الميزات وهي كالتالي :

- يزودك هذا السيرفر بإمكانية تزويد كل مستخدم باسم مستخدم وكلمة مرور, والتي يمكنك تفعيلها عن طريق الـ Hostspot . ويتميز الهوت سبوت بالكثير من الميزات, وأهمها عرض صفحة إعلانية للمستخدمين, وتحتوي على حقل اسم المستخدم وكلمة المرور كما هو موضح في الصورة التالية :



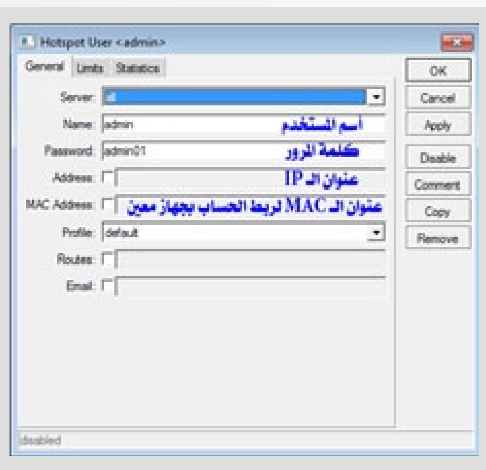
- من خلال سيرفر المايكروتك ، يمكنك أيضاً دمج عدة خطوط إنترنت وإخراجها بسرعة خط واحد . وهذه الميزة مفيدة جداً لأصحاب الشبكات ذات العدد الكبير من المستخدمين. ففي حال استأجروا أقصى سرعة من مزود الخدمة ورغبوا مستقبلاً بسرعة أكبر ، يمكنهم استئجار خط آخر من مزود خدمة آخر ثم دمج هذان الخطان مع بعض لإخراجهم بسرعة خط واحد . وهذا سيمكّنهم من زيادة عدد المستخدمين . والصورة التالية توضح عملية إدخال وإخراج الخدمة في السيرفر :



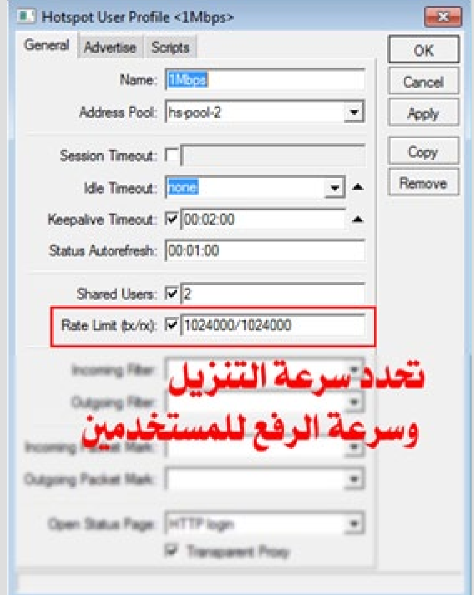
- إدراة المستخدمين :

كما تعلم أنّ إدارة المستخدمين هي من أهم الأشياء التي يقدمها السيرفر . ولكن الوضع مع سيرفر المايكروتك مختلف تماماً عن بقية السيرفرات . فهو يزودك بميزات كثيرة جداً ونذكر لكم بعضها :

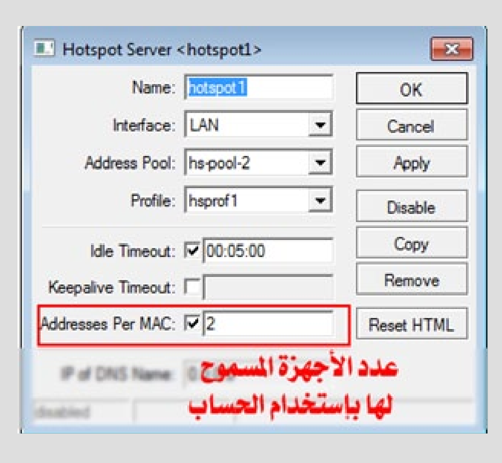
- تحديد اسم مستخدم وكلمة مرور و IP Address لكل مستخدم وربط كل ما سبق بـ MAC Address الخاص به, بحيث لا يستطيع أي أحد من استخدام هذا الحساب إلّا من خلال الجهاز المربوط به الحساب, و لو قام أي شخص بسرقة اسم المستخدم وكلمة المرور الخاصة بك فلن يستفيد شيء .



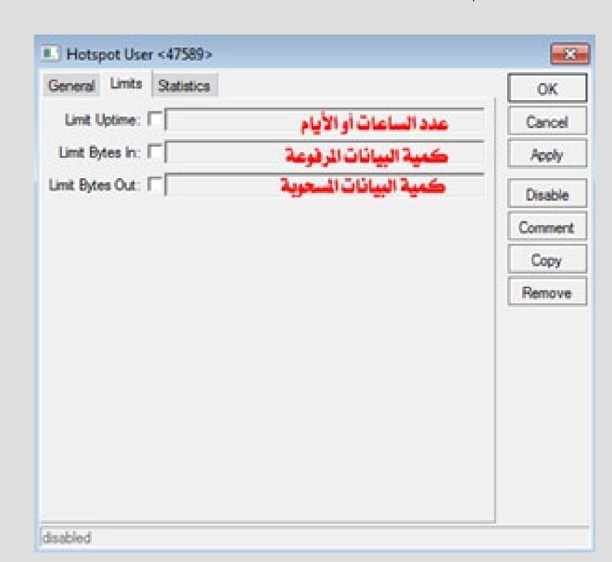
- تقسيم سرعة الإنترنت بين المستخدمين مع إمكانية تقسيم السرعة إلى مجموعات, بحيث تأخذ كل مجموعة سرعة مختلفة .

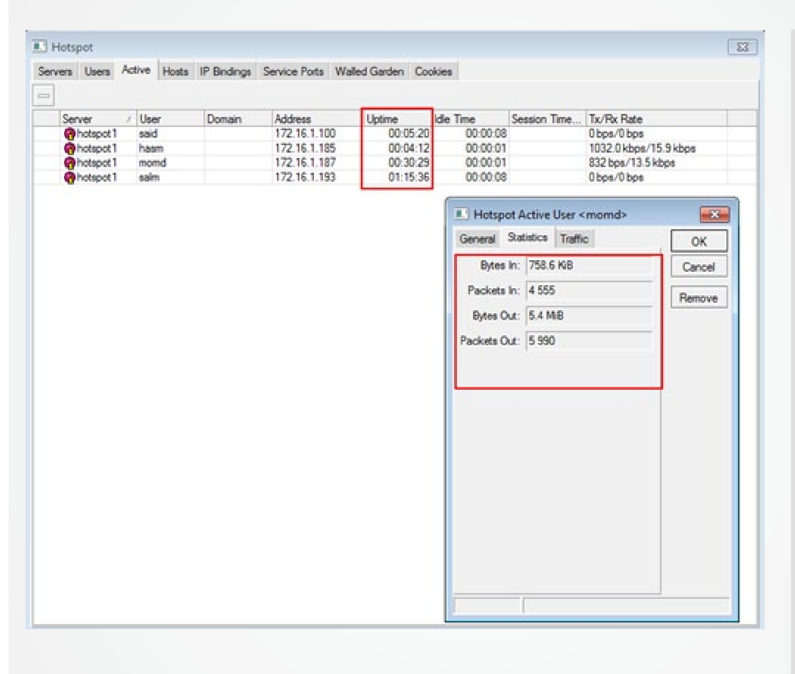


- تحديد حساب لكل عدد من المستخدمين, بحيث يمكنك منع أي مستخدم من استخدام حسابه في أكثر من جهاز في نفس الوقت .

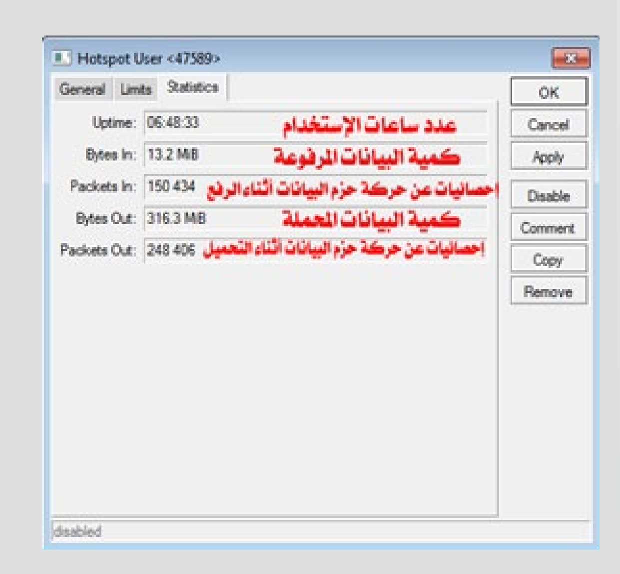


- تحديد اشتراك بالساعات أو اشتراك عن طريق تحديد كمية التحميل ورفع البيانات للمستخدم, وبعد تجاوزها تغلق الخدمة تلقائياً.

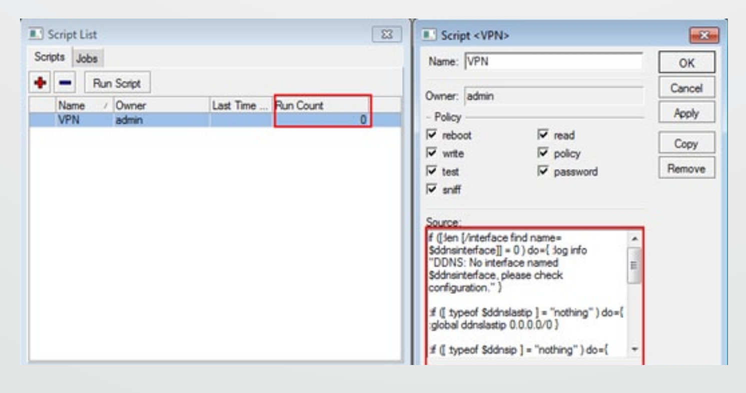




- يوفر لك السيرفر أيضاً إحصائيات عن المستخدمين وعن عدد ساعات استخدامهم واستهلاكهم للبيانات .

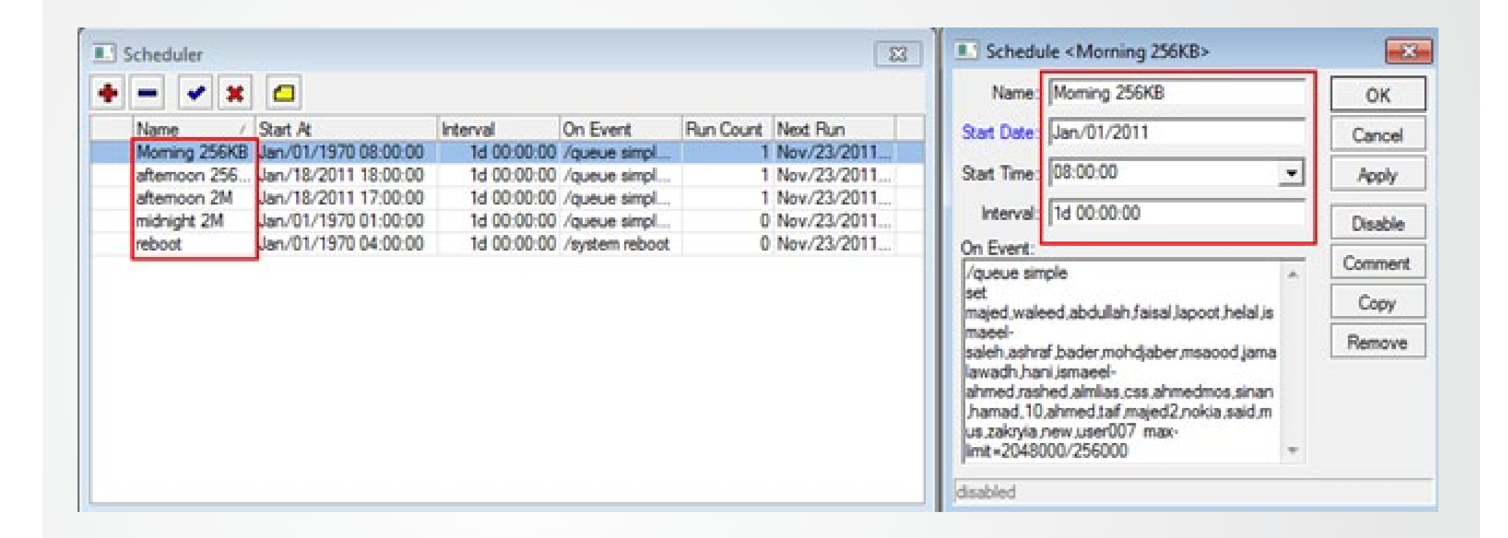


- كما يوفر لك هذا السيرفر لغة برمجة يمكنك استخدامها لإعداد السيرفر أو لكتابة سكربتات لتشغيل خدمات أخرى . كما يمكنك إعداد سكربتات متقدمة تقوم بإدارة السيرفر تلقائياً في حال عدم تواجدك, هنالك أيضاً عدّاد خاص يُظهر فيها عدد المرات التي تنفّذ فيها السكربت, بحيث يمكنك معرفةَ ما إذا كان السكربت لا يعمل بشكل دوري .

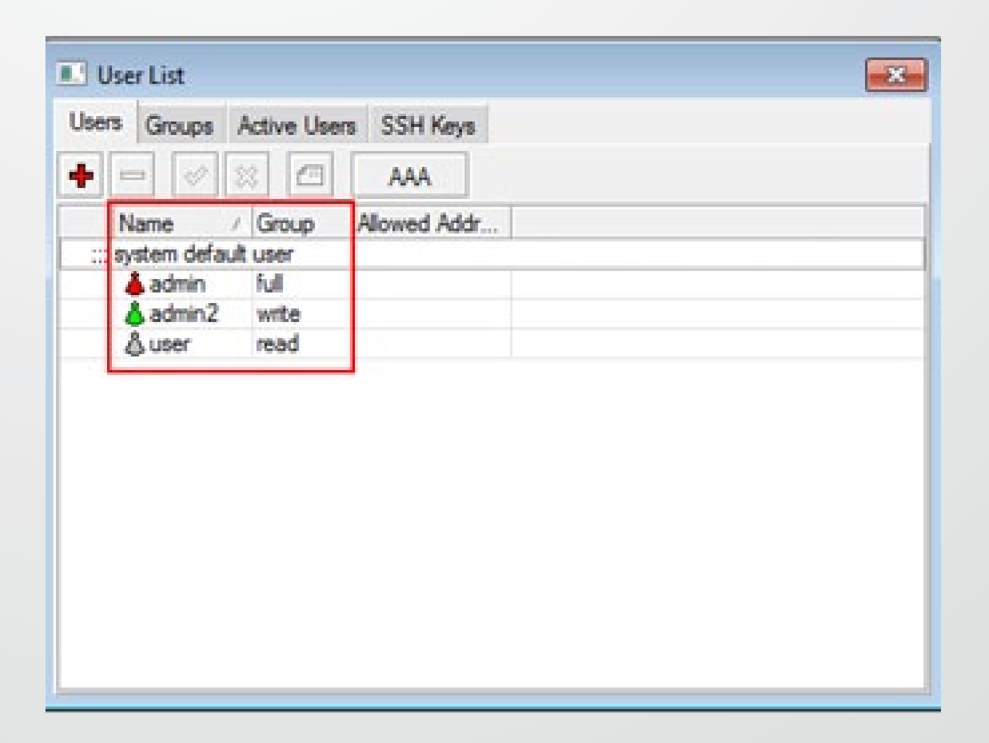


- توجد هنالك أيضاً ميّزة معرفة المستخدمين المتصلين بالشبكة والوقت الذي قضوه على الشبكة, وكذلك البيانات التي رفعوها وحملوها منذ بداية اتصالهم.

- ومن الأمور المتقدمة في هذا السيرفر ، هي وجود Scheduler أو خاصيّة الجدولة, والتي تتيح لك تنفيذ الأوامر في أي وقت تحدده أنت . فمثلاً: يمكنك تقسيم سرعة الإنترنت إلى سرعة مختلفة في النهار وسرعة مختلفة في الليل, أو أن تحجب الخدمة عن مستخدم وقت النهار
وتفتحها وقت الليل, أو أي خدمة تحتاج تنفيذها في وقت معيّن .



- والخاصية الأخيرة والتي نحب أن نتكلم عنها والموجودة في معظم السيرفرات ، هي صلاحيات مدراء السيرفر. فإنّ نظام المايكروتك يوفر صلاحية read only وهي تمكّن مدير السيرفر من القراءة أو النظر إلى السيرفر دون القدرة على تعديل أي شيء, وهنالك صلاحية write وهي تمكّنك من التعديل ولكن ليس كل شيء . أمّا صلاحية Full فهي تمكنك من فعل أي شيء على السيرفر .



هذا ما لدينا اليوم عن سيرفر المايكروتك . وتذكر أيها القارئ أنّ سيرفر المايكروتك يحتوي على ميّزات كثيرة جداً في مجال إدارة خدمة الإنترنت . وتستطيع أن تطلق على نفسك بأنّك مزود لخدمة الإنترنت بمنطقتك عندما تتعامل مع عدد كبير من المستخدمين وتدير خدمة الإنترنت وتوزعها بينهم بطريقة احترافية من خلال سيرفر الفخامة (مايكروتك) .



10 أخطاء يجب تجنبها عند تشغيل الكابلات في شبكتك

في البداية يجب أن تَنتبِه بأنّ الكابلات المُثَبّتة في شبكتك بشكل غير صحيح يُمكِن أن تَشَلُل أداء الشبكة وتعرضك لتكاليف خفية لا تُدركها, كما أنّها تُعرضك للقيام بعملية الـmaintenance (الصيانة) بشكل دوري بسبب ظهور مشاكل مستمرة في الكابلات تُعطّل أداء العمل في مُنظمتك.

لذلك أحببت أن أعرض لكم الأخطاء العشرة التي يجب أن تتجنبها عندما تقوم بتشغيل الكابلات في شبكتك حتى تستطيع القيام ببناء شبكة سليمة منظّمة لا تُكلفك الكثير من الوقت والمال في المستقبل.

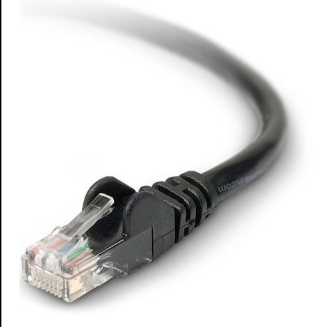


1 الخطأ الأول

عدم التخطيط للمستقبل

ربما تكون المنظمة التي تعمل بها تستخدِم في الـ network كابلات سرعة الاتصال بها Mbps100 لأجهزة الـdesktop , مثل الـ (laptop-PC), وتكون هذه السرعة من الشروط أو من ضمن البنود المسبقة عند بناء هذه الشبكة, وبالتالي فأنت مُجبَر بها في الوقت الحالي ، وبذلك حتى لو أصبحَت سرعة الاتصال 1 Gbps هي الأكثر قياسية في هذه الشبكة أي (pretty standard) فأنت لا تستطيع تغيير الكابلات من الـ Mbps100 إلى Gbps 1.

مثال للتبسيط: لديك أجهزة في الشبكة كانت تعمل في البداية بسرعة Mbps100, وبالتالي فأنت تستخدم كابلات بسرعة Mbps100, ولكن إذا تم تغيير كروت الـ network في أجهزة الـ desktop إلى كروت شبكة تعمل بسرعة 1000/100/10 Mbps , فالسؤال الآن, ما هو أفضل كابل للاستخدام لتحقق أعلى سرعة ممكنة؟هل تستخدم كابلات بسرعة 10Mbps؟ أم 100Mbps؟ أم 1000Mbps؟ بالطبع تقوم باستخدام كابلات تسير بسرعة 1000 ميجا بالثانية (1Gbps), وبالتالي تقوم باستخدام standard متماثل في شبكتك يحقق لك أعلى سرعة ممكنة.






ومن المثال السابق نجد أنّ هناك مشكلة تواجهك وهي بعدم قدرتك على تغيير جميع هذه الـcables لأسباب كثيرة, منها التكلفة والوقت وغيرها من الأسباب الأخرى التي نعلمها،ولكن لنفترض أنّ منظمتك سوف تتوجه لبناء موقع جديد وكَلّفتك ببناء شبكة بها كابلات جديدة, فمن الطبيعي هل ستقوم باختيار أفضل cabling technology كانت تُستخدَم بالأمس ؟ أم تقوم باختيار cables تُستخدَم في الأيام الحالية وتُلبي إحتياجات شبكتك و مُنظمتَك وتَصلُح للاستخدام للسنوات القليلة القادمة؟ بالطبع سيكون خيارك هو الثاني.

ولكن يجب أن تأخذ في اعتبارك أنّ الكابل الذي يحقق لك أعلى كفاءة لن يكون الخيار صاحب أقل تكلفة, لذلك ينبغي عليك أن تنظر إلى الكابلات ذات التكلفة المعقولة نوعاً ما, وكذلك تؤدي أعلى كفاءة لمنظمتك. فمثلا نجد العديد من المنظمات لن تحتاج إلى كابلات بسرعة 10Gbps لأجهزة الـdesktop , وليس معنى ذلك أن نذهب لشراء الكابلات الرخيصة التي لا تناسب شبكتك لإرضاء منظمتك, وإنّما تقوم بشراء الكابلات وفقاً للاحتياجات التي تناسب شبكتك وتكلفة منظمتك.

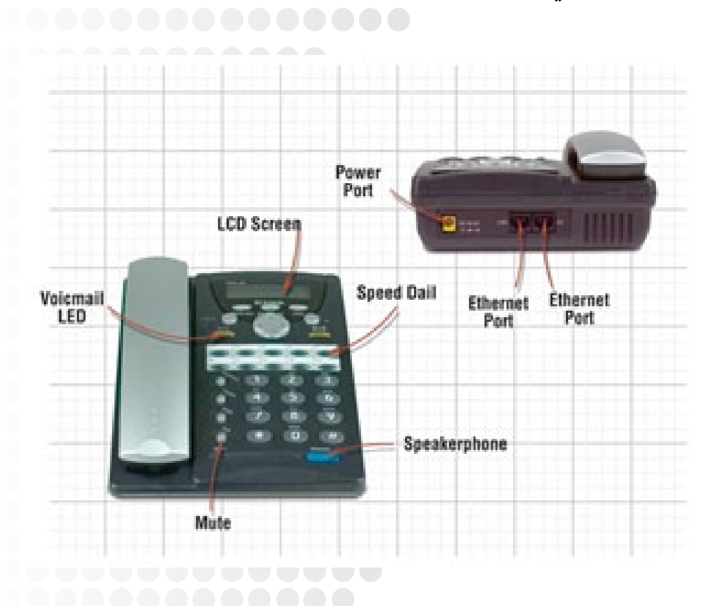
فاختيارك يترتب بناءً على التكلفة ونظرتك المستقبلية, ويجب أن تتذكر دائماً بأنّ العمل للتخطيط للمستقبل هو أغنى وأهم جزء في المشروع الذي تقوم بتنفيذه.

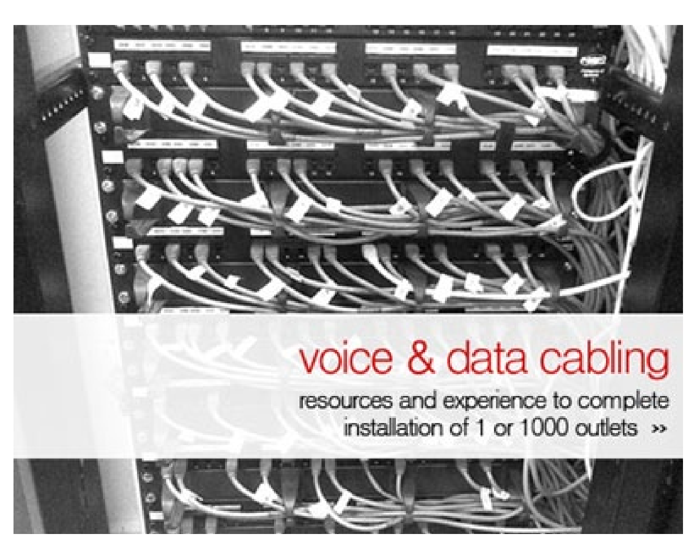


استخدام كابلات مختلفة لنقل كُلاً من الـ ((voice والـ data)

حقيقةً, إنّ كابلات الـ Twisted pair في بداية ظهورها كانت تكلفتها مُرتفعة نوعاً ما, وبالتالي كانت تلجأ بعض الشركات إلى استخدام كابلات مختلفة لنقل كلاً من الصوت والبيانات وبتكلفة أقل من كابلات الـ Twisted pair, ولكن وجدت هذه الشركات أن خدمة الصوت التي تقدمها أقل ما يمكن ويصعب إرضاء العميل بها, لأنّ الصوت يتطلب فقط زوج واحد من الأسلاك (Twisted pair)، ثم بعد ذلك توجهت هذه الشركات إلى استخدام كابلات أقل تكلفة لنقل الصوت في حين أنّ البيانات في وقتها كانت تُنقل في كابلات تحمل ميزانية مرتفعة.

ومع التقدم التقني والتطورات اليومية التي نلاحظها اليوم فيمكنك أن تقوم بتثبيت كامل (complete installation) في شبكتك لا يحقق لك تكلفة عالية سوى تكلفة العمالة, لأنّ الكابلات التي تقوم باستخدامها لا تُعتبَر تكلفة ضخمة, لأنّك الآن تستطيع استخدام خدمات مثل خدمة الـvoip التي تنقل لك الصوت عبر الـip وبالتالي توفر لك الكثير من التكلفة.

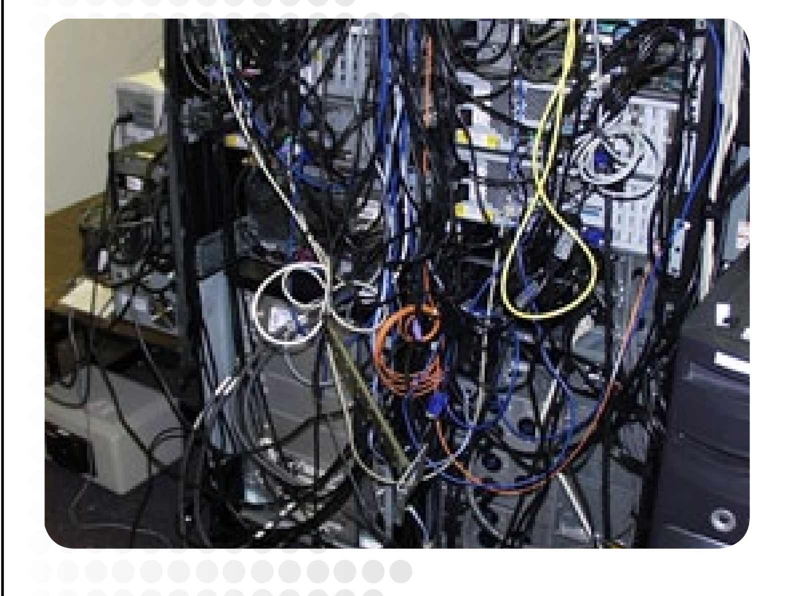




ومن المثال السابق نجد أنّ هناك مشكلة تواجهك وهي بعدم قدرتك على تغيير جميع هذه الـcables لأسباب كثيرة, منها التكلفة والوقت وغيرها من الأسباب الأخرى التي نعلمها،ولكن لنفترض أنّ منظمتك سوف تتوجه لبناء موقع جديد ومكاتبك ببناء شبكة بها كابلات جديدة, فمن الطبيعي هل ستقوم باختيار أفضل cabling technology كانت تُستخدَم بالأمس؟ أم تقوم باختيار cables تُستخدَم في الأيام الحالية وتُلبي إحتياجات شبكتك و مُنظمتَك وتَصلُ للاستخدام لسنوات القليلة القادمة؟ بالطبع سيكون خيارك هو الثاني.

ولكن يجب أن تأخذ في اعتبارك أنّ الكابل الذي يحقق لك أعلى كفاءة لن يكون الخيار صاحب أقل تكلفة لذلك ينبغي عليك أن تنظر إلى الكابلات ذات التكلفة المعقولة نوعاً ما, وكذلك تؤدي أعلى كفاءة لمنظمتك. فمثلا نجد العديد من المنظمات تحتاج إلى كابلات بسرعة 10Gbps لأجهزة الـdesktop , وليس معنى ذلك أن نذهب لشراء الكابلات الرخيصة التي لا تناسب شبكتك لإرضاء منظمتك, وإنّما تقوم بشراء الكابلات وفقاً للاحتياجات التي تناسب شبكتك وتكلفة منظمتك.

فاختيارك يترتب بناءً على التكلفة ونظرتك المستقبلية, ويجب أن تتذكر دائماً بأنّ العمل للتخطيط للمستقبل هو أول وأهم جزء في المشروع الذي تقوم بتنفيذه.



3 الخطأ الثالث

تجاهُل عملية إدارة الكابلات عند إعداد الشبكة

غالباً ما تتجاهل بعض المنظمات عملية إدارة الكابلات, والبعض الآخر ينظر إليه بأنّه شيء هام ويعطي شكلاً جميلاً للشبكة, كما أنّه يُسهّل عملية الصيانة عند وجود مشاكل فنية ،ففي الحقيقة عملية الإدارة من العمليات المهمة التي توفر لك الكثير من التكلفة والوقت عند ظهور مشاكل في المستقبل, وخاصةً إذا كان السيناريو الذي تقوم بإعداده كبير ويحتوى على الكثير من السويتشات و الكابلات, وفي هذه الحالة أنصحك بإضافة أو استخدام (ladder rack), حيث أنّ إدارة الكابلات مُرتبطة بتنظيم الـcables وترتيبها بشكل جيد داخل هذا الـ rack

الـ (ladder rack) وهو عبارة عن سلم يجمع أكثر من rack في نفس الوقت, وبالتالي يجعل شبكتك وأسلاكك أكثر تنظيماً كما إنه يجعل عملية الصيانة أكثر سهولة.





وهذه الصور توضح الفرق بين الشبكة التي بها إدارة كابلات والشبكة التي يتم فيها تجاهل عملية الإدارة للكابلات





ملاحظات :

1 - في البداية يجب أن تضع في اعتبارك أنّه لابد من اختبار الكابلات والتأكد من أنّها مناسبة وتؤدي عملها, ولن تتوقف وتعمل بشكل سليم.

2 - التأكد من أنّه سوف يتم إضافة المزيد من الكابلات في المستقبل.

3 - استخدم طرق معينة ومختلفة لتحديد الكابلات, فمثلاً قم بتسمية الكابلات أو استخدم الكابلات الملونة أو التي بها رموز أو غيرها من الطرق التي تناسبك وتسهّل عليك التعرف على الكابلات التي تديرها في وقت لاحق.

4 الخطأ الرابع

تشغيل كابلات الشبكة بجانب الكابلات الكهربائية



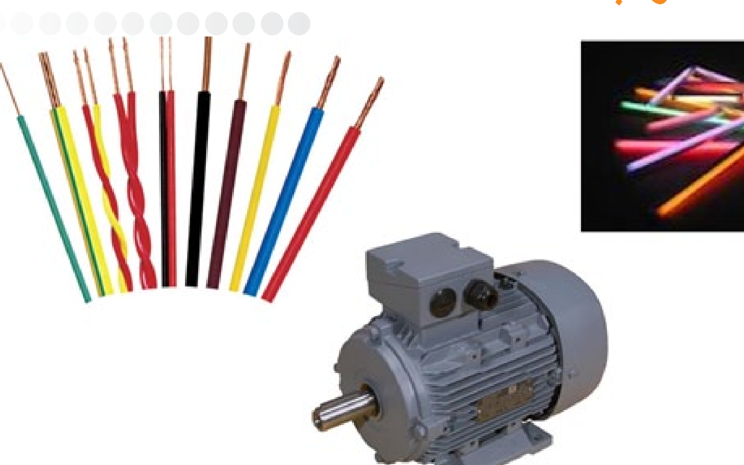
من المعروف أنّ كابلات الـ UTP تُستخدم لنقل البيانات من خلالها،ولكنٍ أغلبنا لا يعرف أنّ هذه الكابلات بها مجال مغناطيسي (magnetic field) يُولِّد جُهد كهربائي مُنخفِض (low voltage) من خلال تشغيل الـ cable.

لذلك عندما تقوم بتشغيل كابلات الـ unshielded بجانب الكابلات الكهربائية يُصبح المجال المغناطيسي الموجود في كابل الـ UTP مُعطَل, لأنّ الكابلات الكهربائية تؤثّر على أداء كابلات الـunshielded وبالتالي يُصبح الـ communication الموجود في الشبكة به نوع من الـ noisy أو التشويش مما يؤدي إلى وجود تقطُّع في الاتصال, ووجود بطء في الشبكة وعدم القدرة على الإرسال من جهاز إلى آخر.

لذلك يُنصَح بأن تُبعِد الكابلات الخاصة بشبكتك عن الأماكن التي تحتوي على كابلات كهربائية أو الأماكن التي بها خطوط الطاقة الكهربائية (electrical power lines).

5 الخطأ الخامس

تشغيل الـ cable بالقرب من devices مزعجة



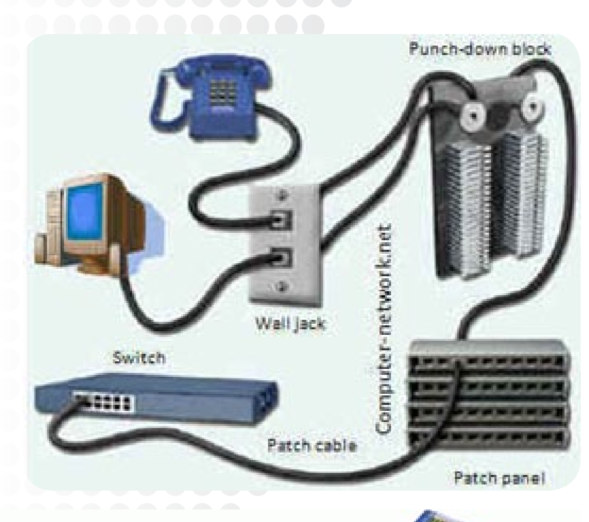
حيث أن الضوضاء تؤثر على مرور البيانات في الكابل, كما أن الأسلاك الكهربائية وإضاءة الفلورسنت (Fluorescent) والمحركات (motors) والـ items المشابهة التي تُحدِث التدخلات الكهربائية أو المغناطيسية سوف تعيث فساداً في كابلات الـ infrastructureالخاصة بك،وبالتالي فعليك التأكد من أن تخطيطك الصحيح يتجنب لك هذا النوع من المخاطر.



عدم التدبير والحساب للمسافات المحددة إلى الـ end point

إذا كلفتك الشركة أو المنظمة التي تعمل بها بتوصيل الكابلات لجميع الأجهزة في شبكة ما. فعليك أن تعرف ما هي المسافة المحددة التي يسير فيها الكابل لكي يصل إلى الـend point ؟, وما هي سرعة الـNIC التي توجد بهذه الأجهزة؟, فإذا كانت كروت الشبكة من نوع الـ Ethernet (أي تسير بسرعة 10Mbps) حتى الـ GigaEthernet (أي تسير بسرعة 1Gbps) والمسافة لا تزيد عن 100 متر فأنت بحاجة إلى استخدام كابل من نوع UTP، أما إذا كنت تقوم بتشغيل الكابلات لبعض الأغراض الأخرى (أي لمسافات بعيدة وسرعات عالية) مثل 10 جيجابايت في الثانية أو 40 جيجابايت في الثانية، فيجب أن تضع في اعتبارك قيود المسافة المقترنة مع أي نوع من الكابلات سوف تنوي استخدامه في هذه الحالة.

فعلى سبيل المثال: لو أردت تشغيل شبكة بسرعة 10Gbps ولمسافة تزيد عن 100 متر فأنت بحاجة إلى استخدام cable من فئة الـ Category 6A أو cable أفضل منه لكي تحصل على أكثر كفاءة وسرعة ممكنة.







عدم اتّباع القوانين

إفاتّباع القوانين المحلية الخاصة بشركتك من الأشياء الهامة التي يجب الالتزام بها, كما أن عدم الالتزام والتقيد بالقوانين سوف يؤدي ذلك إلى مشاكل خطيرة منها التأثير على سلامة وأمان الموظفين.

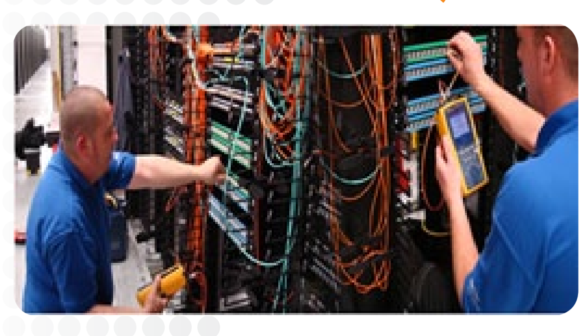
مثال: في أغلب الأماكن المعرضة للهواء يحظر تغطية الكابلات بأشياء بلاستيكية (PVC-jacketed cabling) لأنّها إذا تعرضت للحريق سيُصبح أمراً صعباً على رجال الإطفاء لأداء مهمتهم في الإطفاء, كما أنَّ الموظفين قد يضطروا إلى التنقل لمنطقة أخرى في حالات حدوث الطوارئ.

مثال أخر: إذا كنت لا تتبع القوانين المحلية المُتعلِقة باستخدام كابلات ذات جهد منخفض (low voltage) فسوف تواجه خطر الغرامات وربما حتى لاستبدال جميع التجهيزات والكابلات الخاصة بك التي قمت بإعدادها في البداية .لذا تأكد وتحقق من المسؤوليات الخاصة بك قبل البدء وتأكد من أن المقاولين العاملين لديك مدركين أيضاً بنفس القوانين التي تملكها وتسير عليها.



8 الخطأ الثامن

عدم اختبار كابلات الـ infrastructureالخاصة بك



قبل تثبيت الكابلات في الشبكة يجب اختبار كل cable باستخدام الأدوات المناسبة للتأكد من أنّ هذه الكابلات تكون مناسبة وصالحة للاستخدام المقصود منه، وهذا الاختبار يشمل طول الكابل وذلك بالتحقق من مطابقة المواصفات والاحتياجات.

فعلى سبيل المثال: إذا كنت بحاجة إلى سرعة اتصال وإرسال تصل إلى1Gb في الثانية فتأكد من أنّ خصائص وطول الكابل سوف يدعم ذلك أم يحتاج إلى دعم.





9 الخطأ التاسع

عدم اتّباع الـ standard

كما تعلم أنه يوجد ثمانية أسلاك فردية داخل الـ cable, فبعضنا يقوم بترتيب هذه الأسلاك وتوصيلها بطريقة عشوائية ولا نطبّق الـ standard الخاص بترتيب الأسلاك ترتيب معين, ولا نُدرك بأنّ معظم الـ devices في الشبكة مثل روترات وسويتشات سيسكو لا تقوم بعملها إلّا بتطبيق هذا الـ standard، لذلك يُفضّل أن تسير على standard ثابت يضمن لك العمل بدون مشاكل وبأكثر كفاءة ممكنة. فإذا اعترضت وخالفت هذه الـstandard فسوف تقع في مشاكل يمكن أن يكون لها أثر سلبي على أداء الشبكة ككل.

فيوجد standard معروف لترتيب الأسلاك ويتم هذا الترتيب بناءاً على نوع الجهازين المُتصلين ببعضهم:

1 - إذا كان الجهازين المتصلين ببعضهم (MIDI) مثل الـRouter و الـ PC, فيتم توصيلهما بكابل UTP أسلاك مرتبة بطريقة Cross over.

2 - إذا كان الجهازين المتصلين ببعضهم (MIDIX) مثل الـHub و الـ Switch, فيتم توصيلهما بكابل UTP أسلاكه مرتبة بطريقة Cross over.

3 - إذا كان الجهازين المتصلين ببعضهم أحدهم (MIDI) والآخر(MIDIX) مثل الـ PCوالـ Switch, فيتم توصيلهما بكابل UTP أسلاكه مرتبة بطريقة Straight-through.



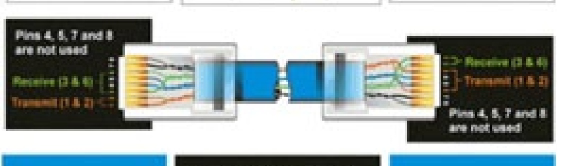


Straight-Through

Pin number	Wire Color
Pin 1	Orange/White
Pin 2	Orange
Pin 3	Green/White
Pin 4	Blue
Pin 5	Blue/White
Pin 6	Green
Pin 7	Brown/White
Pin 8	Brown

Wire	Becomes
1	1
2	2
3	3
6	6

Pin number	Wire Color
Pin 1	Orange/White
Pin 2	Orange
Pin 3	Green/White
Pin 4	Blue
Pin 5	Blue/White
Pin 6	Green
Pin 7	Brown/White
Pin 8	Brown



Crossed-Over

Pin number	Wire Color
Pin 1	Orange/White
Pin 2	Orange
Pin 3	Green/White
Pin 4	Blue
Pin 5	Blue/White
Pin 6	Green
Pin 7	Brown/White
Pin 8	Brown

Wire	Becomes
1	3
2	6
3	1
6	2

Pin number	Wire Color
Pin 1	Green/White
Pin 2	Green
Pin 3	Orange/White
Pin 4	Blue
Pin 5	Blue/White
Pin 6	Orange
Pin 7	Brown/White
Pin 8	Brown

10 الخطأ العاشر

عدم تشغيل الـ cables التي تحتاجها



وأخيراً إنتقلنا إلى الخطأ العاشر والأخير الذي يكون غامضاً نوعاً ما عند قراءة عنوانه, ولكن سوف أقوم بشرح ما أريد توضيحه في السطور التالية:

تخيل معي لو أن لديك في شبكتك (Ethernet switch) وكابلات Ethernet وأخرى Fast Ethernet ففي هذه الحالة ما هو نوع الكابل الذي سوف تقوم باستخدامه؟.هل تستخدم الـ Ethernet؟ أم الـFast Ethernet ؟ , ولماذا؟

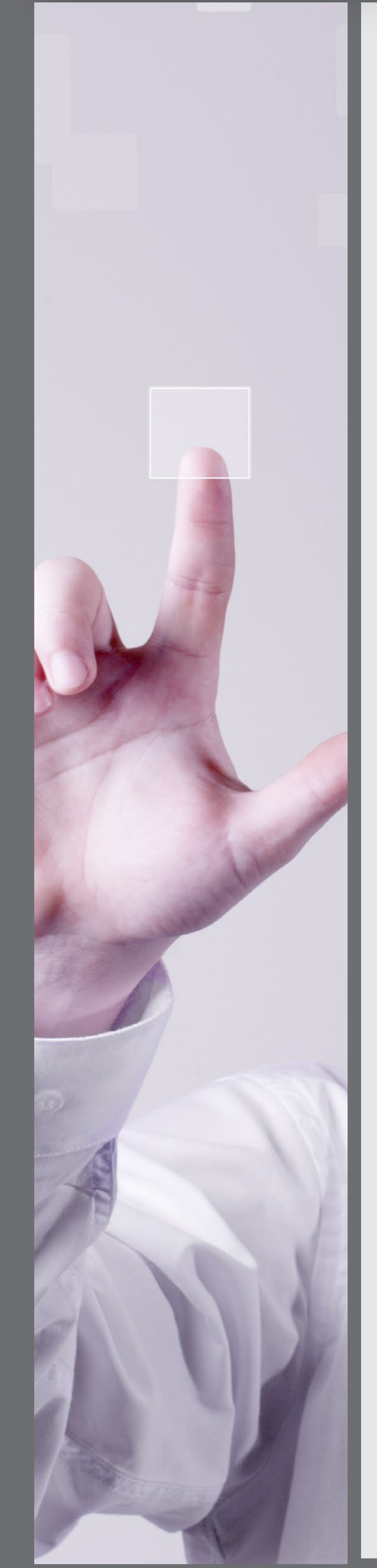
الإجابة: بالطبع سوف تستخدم كابلات الـEthernet، لأنـّك مُخضَع لسرعة الجهاز المتصل به, هل هو يفهم سرعة الـ (Ethernet 10Mbps ؟ أم يفهم سرعة Fast Ethernet) 100Mbps)؟. كما أنـّك استخدمت الـcable المناسب وفق احتياجات شبكتك والذي يحقق لك الكفاءة المطلوبة ويجعل شبكتك تسير بشكل من منتظم.

ولكن إذا قمت بتشغيل كابل بسرعة Fast Ethernet) 100Mbps) فسيؤدي ذلك إلى حدوث مخاطر مثل عدم الاستقرار في الشبكة (instability) وحدوث اختناقات في الشبكة غير مُرتب لها من قبل, وبالتالي فأنت تقع في هذا الخطأ المذكور أعلاه ألا وهو (عدم تشغيل الـ cables التي تحتاجها).

وفي النهاية أتمنى أن يكون الموضوع قد نال إعجابكم ولا تنسوني من صالح دعائكم،وفي لقاء قادم إن شاء اللّه.



نظرة عامة حول
IPv6 multicasting



- Multicast Listener Discovery

Multicast receivers يجب أن تُبلّغ Gateway router بأنّها تريد استقبال multicast ترافيك لـgroup أو مجموعة ما. تقوم الـ hosts بتبليغ الروتر عن طريق بروتوكولMLD (Multicast Listener Discovery) .

قام IPv6 multicast بتسميةIGMP إلىMLD ، النسخة الأولى منMLD هي شبيهة لـ IGMP v1 ، بينما النسخة الثانية من MLD هي شبيهة لـ MLD v2، IGMP v2 تدعم SSM) Source Specific Multicast) ، حيث يمكن لـ Host أن يحددSources الذي يود أن يستقبل الترافيك منها بالنسبة لـ Group ما.MLD v2 متوافق معMLD v1 , يستخدمMLD بروتوكول ICMP) Internet Control Message Protocol) لنقل رسائله .

يستخدمMLD ثلاثة أنواع من الرسائل:Report، Query ، و . Done MLD Done messageمثل Leave message في IGMP v2.

فهو يشير إلى أنّHost ما لم يعد يرغب في تلقي الـ multicat ترافيك لمجموعة ما . أمّا message Query يرسله الروتر بشكل دوري لتحديد ما إذا كان أيhost يرغب في استقبال الـ multicast ترافيك لـ Group ما. Report messageيرسلهhost لإعلان رغبته بأنّه يريد استقبال multicast ترافيك لـ Group ما.

MLD Snoopingيوفر نفس الوظائف مثل IGMP Snooping فيIPv4 . ، فهو يوفر معلومات لـ Switch حولconnected hosts التي هي عضو في مجموعة معينة, بحيث يمكن لـ Switch اتخاذ قرارات بشأن Interface التي سيرسل لها الـmulticast ترافيك.

- Protocol Independent Multicast

PIM) Protocol Independent Multicast) يستخدم بين الروترات، بحيث يمكّنهم من تتبع أي من حزم الـ multicast يجب أن يرسلوها بينهم ، لإرسالها إلى الشبكات المحلية. يعملPIM بشكل مستقل عن بروتوكول unicast routing للقيام بإرسال أو تلقيmulticast update route مثل البروتوكولات الأخرى.

IPv6 PIM يدعم 2 SM) sparse mode ، modes) وsource-specific multicast (SSM) ، IPv6 PIM لا يدعم Dense Mode مثل IPv4 PIM . IPv6 PIM يتطلب إعدادstatically (RP) Rendezvous Point فيRP router .

Magazine

NetworkSet